RILA
RETAIL INDUSTRY LEADERS ASSOCIATION

1700 N. Moore Street, Suite 2250, Arlington, VA 22209

June 15, 2018

U.S. Consumer Product Safety Commission
Office of the Secretary
Room 8204
330 East-West Highway
Bethesda, MD 20814

RE: The Internet of Things and Consumer Product Hazards, Docket No. CPSC–2018–0007

Dear Madam Secretary:

The Retail Industry Leaders Association (RILA) appreciates the opportunity to expand on our testimony of May 16, 2018 at the U.S. Consumer Product Safety Commission (CPSC) hearing on the Internet of Things and Consumer Product Hazards (IoT Hearing). By way of background, RILA's members include the largest and most innovative retailers. The retail industry employs over 42 million Americans and accounts for $1.5 trillion in annual sales. RILA members strive to provide American consumers with a wide variety of safe and innovate products. As technology continues to evolve, so do RILA member's offerings.

The initial comments and testimony provided by RILA at the IoT Hearing outlined suggestions under three categories – Education, Collaboration and Engagement – for action steps the CPSC could take to enhance the safety of IoT products. Those suggestions and action steps are important starting points. These comments will expand upon our prior testimony and provide some additional suggestions. We look forward to continuing to work with the CPSC on our shared product safety goals. A summary of our comments is below.

Executive Summary

RILA's comments are divided into three topic areas: 1) discussion of the current landscape and challenges in regulating internet-connected (IoT) products; 2) suggestions on how the CPSC can engage on this issue; 3) and ways retailers can support the CPSC as the agency looks to get involved in learning about IoT products. The major discussion points within these topic areas are summarized below.

First, an ever-increasing number of innovative IoT products provide tremendous benefits and convenience to consumers. IoT technology and products also come with potential security, privacy and safety risks and other challenges including lack of clarity regarding lines of various federal agencies' jurisdiction.

Second, any future CPSC action related to IoT products should fall within the bounds of its statutory authority. Establishment of interagency protocols will enable the CPSC to collaborate with other federal agencies in situations involving product failures across multiple risk areas.

Third, the CPSC should expand its participation in joint federal agency efforts and intergovernmental groups as well as increase its international collaboration and cooperation efforts on IoT technology and products.

Fourth, the CPSC should continue to rely on voluntary standards as an effective means of protecting the safety of consumers while encouraging product innovation. In addition, the agency should look to the example of other federal agencies when considering development of any potential voluntary IoT product safety guidance.

Fifth, there is a critical need to enhance CPSC staff expertise, experience and skills in IoT and other emerging technologies.

Lastly, RILA and its members support the CPSC's effort to enhance the safety of IoT products and urge the agency to expand and formalize the Retail Reporting Program as a government/industry partnership program to enable retailers and other stakeholders to provide the CPSC with real-time IoT product specific incident data.

Each of these points is discussed in more detail below.

I. The Current Landscape of IoT Technology and Products

As the testimony at the IoT Hearing revealed, IoT technology is new, emerging and rapidly changing. New innovative IoT products are coming on the market daily and the potential uses of IoT technology are almost endless. Today, IoT technology is in everything from fantastical driverless cars, medical breakthrough pacemakers, and smart refrigerators. These products promise tremendous potential safety benefits and consumer convenience and are just the tip of the iceberg as to the kind of products that will have IoT technology in the future.

Federal regulatory agencies are struggling to understand the nature of the technology and potential risks related IoT technology and products.[1] Multiple regulatory agencies have concurrent and complementary jurisdiction over IoT technology and products and there is a need for clarity as to the exact lines of agency jurisdiction.[2] In addition, there is a need for a single

[1] For example, there is no agreed up definition of Internet of Things (IoT). In the Federal Register notice for the IoT Hearing, 83 Fed. Reg. 13123, CPSC defined IoT as, "products with a connection to the internet that can transmit or receive data, upload or download operating software or firmware, or communicate with other internet-connected devices." Whereas, the Government Accountability Office (GAO) defines IoT as:

> The Internet of Things (IoT) generally refers to the technologies and devices that allow for the network connection and interaction of a wide array of devices, or "things," throughout such places as buildings, vehicles, transportation infrastructure, or homes. IoT devices, or "smart" devices, are increasingly being used to communicate and process information to an extent that was not possible before. (U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-17-570, COMMUNITIES DEPLOY PROJECTS BY COMBINING FEDERAL SUPPORT WITH OTHER FUNDS AND EXPERTISE, (2017).)

While these definitions are similar, they are not the same and as a result could lead to different outcomes in IoT policy, standards and regulations. Developing a common definition of IoT will be critical as federal agencies continue to collaborate on IoT policy and work toward coordinated goals.

[2] For example: the National Institute of Standards and Technology (NIST) is currently working on government/industry cybersecurity standards; the Federal Trade Commission (FTC) has statutory jurisdiction over

coordinated approach and aligned policy goals and objectives among federal agencies regarding IoT policy. At the same time, the nature, capabilities and risks related to individual IoT products varies greatly and, as a result, there is no one-size-fits-all solution for regulating internet-connected products. IoT technology in products raise new and unique challenges and RILA applauds the CPSC for engaging on this issue and reviewing this technology to see where the agency has a role to play to enhance the safety of these products.

A. IoT Products Offer Potential Safety, Consumer Convenience, and Industry Efficiency Benefits

IoT products have the potential to provide benefits that will directly impact consumers lives in very positive ways. Connected baby monitors can alert parents when a newborn baby is in distress and has stopped breathing. Smart smoke alarms can warn consumers when the batteries should be changed (without that annoying and inevitable middle-of-the-night chirp). Smart bike helmets can alert emergency personnel if the rider gets into an accident.

Another major safety benefit of IoT technology is that manufacturers will have the ability to address a potential safety issue before an incident has even happened. Many times, if a potential safety issue related to IoT technology software is identified, it can be quickly and easily addressed via a software patch that is pushed out to the product. That potential to fix a hazard, with little to no adverse impact on the consumer, is groundbreaking and is something that the CPSC staff has identified as a significant potential safety benefit of IoT technology.[3]

Subject to applicable consumer privacy and consent requirements, manufacturers' ability to collect data on product use, and even misuse, is another potential benefit of smart products. Product data can be used to inform updates to products and potential product research and development in the future. If manufacturers can in real time, over multiple users see use and hazard patterns, they can be much quicker identifying and addressing potential safety problems.

In addition, product recalls could be closer tracked and consumers could directly be notified using IoT technology. Many IoT consumer products need to be registered to function. As a result, manufacturers may have the ability to directly notify a consumer if that connected product is the subject of a recall, through email, text, on-screen notification, direct mail, and/or social media notifications. Instead of merely relying upon press releases, store posters, or recalls announced on the nightly news to inform consumers about a product recall, direct consumer notification related to IoT products will most certainly increase the likelihood that the consumer has been made aware of the recall notice. IoT technology could go a long way to enhance consumer notification and increase recall effectiveness.

IoT products also offer consumers convenience and efficiency benefits. For example, some internet-connected products can use artificial intelligence (AI) to learn over time. These products

---

privacy and data security; the Food and Drug Administration (FDA) regulates medical devices; National Highway Transportation Safety Administration (NHTSA) is working with car and truck manufacturers on the development of autonomous vehicles; and the Federal Communications Commission (FCC) has jurisdiction over radio frequencies a critical component of IoT technology and products.

[3] U.S. Consumer Product Safety Commission, *Potential Hazards Associated with Emerging Technologies*. January 18, 2017 (Emerging Technologies Report).

can learn a user's house temperature preference and adapt accordingly. Not only is this a comfort and convenience feature, but it also can create energy savings for consumers as smart heating and air conditioning systems can turn off when there is no need to heat and/or cool the house. Another touted benefit is the ability of smart home security devices with cameras to notify consumers when someone is at the door and provide the ability to view the door from a mobile device. Smart refrigerators can help eliminate food waste and streamline daily meal preparation by evaluating ingredients in a refrigerator and suggesting meal recipes. Connected IoT ovens can even detect what is being cooked and can provide suggestions on how to make it by alerting consumers to timers and temperatures.

Businesses too will benefit from use of IoT technology. Just within the retail industry, the worldwide market for IoT hardware for retail applications, including sensors, RFID tags, beacons and wearables, is expected to be worth more than $94 billion by 2025.[4] IoT technology also has the potential to dramatically change manufacturing and sourcing practices. Manufacturers will be able to use IoT technology to reduce waste in the manufacturing process. Also, manufacturers and retailers will be able to track individual products, and even components of products, throughout supply chains and will have the ability to determine the amount of time a product was warehoused and even the temperature of the warehouse. This ability to keep close watch on products allows for the quick capture of any foreseeable safety issue that could arise during the transportation process. In addition, transparent and more efficient supply chains can create potential cost savings that can be passed on to consumers.

B. Potential Risks and Jurisdictional Challenges Related to IoT Technology and Products

The internet of things is still a relatively new concept. While the potential benefits of IoT technology imbedded products is great, there are some unresolved challenges. Much is still not known about the technology and the potential security, privacy and product safety risks related to IoT products. In addition, as noted above and below, multiple federal agencies have jurisdiction over some aspect of IoT technology and products. This creates a potentially confusing situation for consumers, manufacturers, retailers and other stakeholders as to which federal agency has jurisdiction, compliance and enforcement responsibility in a situation.

More and more consumers are voting with their pocketbooks in favor of the benefits and convenience provided by IoT products and other products that incorporate emerging technologies. As the number and range of IoT products continues to grow, clarification of agency jurisdiction and establishment of protocols for agency collaboration on assessment and enforcement is critical. Below, RILA has outlined some additional suggestions for the role the CPSC in this area and action steps the agency can take to enhance the safety of IoT products.

II. Potential Role and Suggested Action Steps for the CPSC to Enhance the Safety of IoT Products

[4] *Retail IoT Could be $94 Billion Market by 2015*, Dan O'Shea, Retail Dive, https://www.retaildive.com/news/retail-iot-could-be-94-billion-market-by-2015/525578/ accessed 6/14/18.

A. Any CPSC Actions Related to IoT Products Should Clearly Fall Within the "Lanes" of the Agency's Statutory Authority

RILA members appreciate the CPSC reviewing ways the agency can continue to keep consumers safe when using internet-connected products. Because of the vast capabilities of internet-connected products, many agencies have a role to play in regulating them, including the CPSC. While the testimony during the IoT Hearing raised many potential concerns regarding IoT products, the CPSC must take care not to conflate issues that clearly fall within the agency's statutory authority and those that do not. Many of the concerns voiced during the IoT hearing focused on potential lack of security in the data that is shared through IoT devices resulting in loss of privacy for consumers. The amount of information that is housed on these devices and is shared through the cloud and other mechanisms is vast.[5] The threat of hackers stealing personal data is real, alarming and could cause major damage to consumers. However, as the CPSC correctly noted in the Federal Register Notice for this proceeding, the CPSC has no statutory jurisdiction over privacy data and security. That responsibility belongs to the FTC. Additionally, concerns raised about the risk of financial crimes and public safety crimes such as the exploitation of children for pornography and trafficking resulting from IoT products belong in the jurisdiction of other federal government and state and local law enforcement.

The CPSC does have jurisdiction over the *safety* of consumer products, including IoT products. This is where the CPSC has unique expertise and can play a vital role in assessing IoT product safety risks. Safety risks could arise from the design of an IoT product where the design of the product does not include adequate safety protocols to address potential safety risks resulting from a product being connected to the internet. Failure of IoT software or a software update could also potentially create safety risks for consumers. The CPSC's safety mission relates to physical hazards of consumer products that could result in physical harm to consumers. The CPSC is an agency focused on safety when Americans are using consumer products, not protecting consumers from data breaches or public safety crimes. RILA strongly urges the CPSC to remain focused on product safety issues.

RILA members recognize that there are situations were there may be multiple potential risks related to an IoT product involving several federal agencies. For example, lack of adequate security protocols in an IoT product could provide an opening to malicious hackers resulting on both privacy and product safety risks. Currently, it is not clear whether the FTC or CPSC would take enforcement action in this situation or if the agencies would collaborate on any enforcement action and recall of an unsafe internet connected consumer product. RILA recommend that the CPSC work with agency partners to establish protocols for interagency collaboration on risk assessment and enforcement related to IoT products.

B. The CPSC Should Support Pending Draft Legislation to Provide Clarity on Agency Jurisdictional Boundaries Related to IoT Products

Representative Bob Latta (D-OH) Chairman of the U.S. House of Representatives Subcommittee on Digital Commerce and Consumer Protection under the Energy and Commerce Committee has developed a bipartisan bill entitled the "State of Modern Application, Research, and Trends of

[5] Information that could be compromised include such things as, routines of when consumers leave and arrive back at their homes, medical history or even the ability to track an individual's every move with GPS.

IoT Act" or the "SMART IoT Act," H.R. 6032, [6] which could help provide some clarity on jurisdictional issues. The bill instructs the DOC to review the current swath of products that contain IoT technology, determine the current landscape of standards and regulations are in place, and determine which agency has jurisdiction. The act aims to help Congress, and the various federal agencies, including the CPSC, get a better picture of the range of IoT products currently out in the marketplace, clearly define existing lines of jurisdiction of the relevant regulatory agencies and identify potential gaps. As this bill moves through Congress, we recommend CPSC support these efforts, and once passed, pledge to work with the DOC to identify what IoT products currently exist and determine which government agency or agencies would have jurisdiction over the product.

C. The CPSC Should Expand Participation in Joint Federal Agency Efforts and Intergovernmental Groups on IoT Technology and Products

As noted earlier, multiple federal government agencies are currently developing policies around IoT technology and internet connected products. In fact, a recent GAO report,[7] which studied use of IoT in communities, highlighted actions that eleven different government agencies are taking to support these communities. The CPSC likely was not asked to participate because the report was not focused on IoT consumer products. Nonetheless, the report shows not only the breadth of the support from the federal government for IoT technology, but also the critical need for CSPC to begin engaging with its partner federal agencies on IoT policy.

One opportunity for CPSC to engage with other federal agencies at a policy level is to reach out to the National Telecommunications and Information Administration (NTIA), an agency under the DOC. One possible way for CPSC to get involved with its interagency partners on a policy level could be through NTIA's Office of Policy Analysis and Development (OPAD). OPAD supports the agency's role as the principal adviser to the President on telecommunications and information policy. According to the OPAD website the group, "develops, analyzes, and advocates public policies that promote innovation, competition, jobs, and economic growth for the benefit of American businesses and consumers."[8] This group would be well served by having a product safety expert be a resource to inform IoT policy related to consumer products and we recommend that the CPSC reach out to OPAD to provide that expertise as necessary.

The Interagency International Cybersecurity Standardization Working Group (IICSWG) provides another opportunity for the CPSC to engage with agency partners. This group currently consists of the NIST, the Department of Homeland Security (DHS), the Department of Justice (DOJ) and the Office of the Director of National Intelligence (ODNI). While the IICSWG is focused on cybersecurity issues, it would be a good starting place for the agency to learn about existing federal cybersecurity efforts to protect American consumers.

---

[6] State of Modern Application, Research, and Trends of IoT Act ("SMART IoT Act"), H.R. 6032, 115th Cong., (2018).

[7] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-17-570, COMMUNITIES DEPLOY PROJECTS BY COMBINING FEDERAL SUPPORT WITH OTHER FUNDS AND EXPERTISE, (2017).

[8] Nat'l Telecommunications and Info. Admin., Office of Policy Analysis and Development, June 3, 2018.

[7] Exec. Order No. 13636, 13 Fed. Reg. 78,33 (February 19, 2013).

Lastly, NIST is the federal government agency that is generally seen as taking the lead in the development of a government and industry wide framework for products and devices connected to the internet. In 2013, via Executive Order 13636,[9] NIST was directed to work with stakeholders and rely on industry standards and guidelines to develop a framework for reducing cyber security risks to critical infrastructures. NIST published the initial Cybersecurity Framework in February 2014 and the Cybersecurity Framework 1.1 in April 2018. According to NIST, the Framework aims to:

> provide a common language and systematic methodology for managing cybersecurity risk…including activities to be incorporated in a cybersecurity program that can be tailored to meet any organization's needs. The Framework is designed to complement, not replace, an organization's cybersecurity program and risk management processes.[10]

The NIST Framework has become a leading resource for guidance and best practices on managing cybersecurity risks. As the CPSC becomes engaged on IoT issues, the agency should look to incorporate the NIST Cybersecurity Framework into its product safety risk analysis.

D. The CPSC Can Look to the Example of Other Federal Agencies when Determining How to Best to Provide Guidance to Industry and Consumers

The CPSC is not the only federal agency that is grappling with how to maneuver in this new world of internet connected products and how best to engage with and provide guidance to regulated communities that will minimize cybersecurity, privacy and safety risks related to IoT devices and products. Several other government agencies have established policies or guidelines for IoT products, which focus on mitigating risks while not limiting innovation. For example, the FDA has issued guidance[11] for the interoperability of medical devices, which among other things, includes guidance on product design, risk management, verification and validation, and labeling. The FDA's guidance also encourages the use of consensus standards for product specific concerns.

The FTC also has developed guidance for data privacy and security of internet connected products. In *Start with Security: A Guide for Business*,[12] the FTC stresses the importance of designing with consumer privacy and data security in mind, and developers make sure service providers are implementing reasonable security measures when developing apps, websites and internet-connected products. Similarly, in late 2017, the Department of Transportation and NHTSA issued *Automated Driving Systems (ADS): A Vision for Safety 2.0*[13]to support the development of the ADS technology and provide guidance to stakeholders, regulated community and states. The voluntary guidance, which incorporated feedback received from public comments and congressional hearings, aligns federal guidance with the latest technology development and industry terminology, clarifies federal and state roles going forward, revises unnecessary design

---

[9] Exec. Order No. 13636, 13 Fed. Reg. 78,33 (February 19, 2013).
[10] Nat'l Inst. of Standards and Tech., Uses and Benefits of the Framework, (June 4, 2018).
[11] Food and Drug Admin., *Design Considerations and Pre-market Submission Recommendations for Interoperable Medical Devices*, September 6, 2017.
[12] Federal Trade Comm., *Start with Security: A Guide for Business*, June 2015.
[13] National Highway Transportation Safety Admin., *Automated Driving Systems (ADS): A Vision for Safety 2.0*, September 2017.

elements from safety self-assessment and clarifies guidance process that that entities do not need to wait to test or deploy ADSs.

Each of the above guidance policies recognizes the importance potential benefits of IoT technology for consumers and industry. Each guidance document seeks to mitigate risk while promoting innovation and retaining flexibility to evolve as technology does. In addition, the guidance documents were the result of outreach and engagement with stakeholders and the regulated communities. As the CPSC looks for ways to enhance product safety while not limiting innovation, the CPSC could consider engaging with stakeholders and the regulatory community to develop high-level, non-binding principles or guidance on IoT products. If the CPSC decides to take this approach, like the documents issued by the FDA, FTC and NHTSA referenced above, any guidance developed by the CPSC should aim to mitigate product safety risks while maintaining ample flexibility in how manufacturers create new products.

Another possible approach was detailed in the recent CPSC Emerging Technologies Report,[14] which included a staff recommendation to implement a program similar to one used at Occupational Health and Safety Administration (OSHA). While the OSHA program highlighted in the report is not focused specifically on IoT technology, there are potential benefits to such a program that encourages agency engagement with all stakeholders, including industry. RILA agrees with staff that engagement with stakeholders is critical to ensuring the best product safety outcomes.

E. As the CPSC Engages on IoT Issues, It Should Continue to Rely on Voluntary Standards

The Consumer Product Safety Act (CPSA)[15] mandates that the CPSC rely on voluntary standards unless there is not wide compliance. RILA members strongly urge the CPSC to avoid considering any kind of mandatory standard for IoT products. IoT technology is in its infancy stage. As this technology matures and more products incorporate it, as well as AI and other emerging technologies, new potential safety risks will be identified. Voluntary standards protect consumers while encouraging innovation. The voluntary standards process works well because it brings many stakeholders to the table to discuss how to achieve safety outcomes. Government, manufacturers, retailers, medical professionals, consumer groups, testing labs and others can work toward the common goal of providing safe products for consumers. This collaborative process also enables voluntary standards to be nimble and quickly address a new safety issue that arises through use in the marketplace; something a mandatory rule would certainly take months, if not years, to address.

The CPSC has a long history of working with voluntary standard setting bodies. CPSC staff does an excellent job of participating in the voluntary standards process, and some are even managing standards committees and work groups. We applaud the agency's willingness and dedication to the consensus standards process.

---

[14] U.S. Consumer Product Safety Commission, *Potential Hazards Associated with Emerging Technologies* 16-17, January 18, 2017.
[15] Consumer Product Safety Act of 1972, 15 U.S.C. § 2064(b).

Work on IoT-related voluntary standards is already underway. One standard that has recently been issued is from Underwriters Laboratory, entitled UL 2900-1 Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements.[16] This standard is but one in a growing number of standards being developed on connected products. Currently several government agencies sit on this standard working group. RILA recommends CPSC participate in this voluntary standard process and other IoT-related voluntary standards that will certainly arise in the future.

In addition, many product voluntary standards now have supplemental materials that provide additional stop-gaps for products within the category that are connected to the internet. An example of one such voluntary standard that has worked well to address potential IoT hazards is the standard for connected space heaters, UL standard 1278 for moveable and wall or ceiling hung electric room heaters.[17] The standard's supplemental material related to IoT enabled product requires certain safeguards to ensure the safety of consumers be put in place before a unit can be accessed remotely. Safeguards such as building in a two or three step process before an appliance can be turned on remotely can avoid accidental activation of the product. This is an example of how the consensus voluntary standards process can quickly adapt to market changes and incorporate protections to address IoT-related risks. RILA recommends the CPSC support such product specific efforts, as necessary.

F. The CPSC Should Expand its International Collaboration and Cooperation on IoT-related Issues

The U.S. is a global leader on many issues but especially in the areas of consumer protection and product safety. The world looks to emulate and collaborate with the CPSC on product safety standards. International collaboration and cooperation on the safety of IoT consumer products is critically important. Technology's reach does not stop at the U.S. border. IoT products have the potential to be used in or activated from any country worldwide. Manufacturers should develop IoT products assuming that the product will be used in or activated from many countries and jurisdictions. Therefore, the U.S. and CPSC, should look to coordinate with other countries to develop aligned product safety goals and risk assessment methodologies.

Recently, the CPSC has increased its international presence, outreach, engagement and collaboration by opening an office in China, providing frequent training to international manufacturers and buyers, hosting multi-country safety summits, and engaging with the Organization for Economic Cooperation and Development (OECD), which is made up of representatives from 34 different countries. As the OECD representative testified at the IoT Hearing, the organization is closely following and analyzing IoT product development with a view to developing guidance and a risk assessment methodology and would welcome the CPSC's input. Having the CPSC participate at OECD meetings would allow the agency to gain valuable insight into the risk methodologies and safety measures other countries considering with respect to the IoT devices, while also providing the CPSC the opportunity to share the U.S. learnings from the agency's experiences with these products.

---

[16] Underwriters Laboratories, Inc., UL 2900-1 Standard for Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements, 5 July 2017.
[17] Underwriters Laboratories, Inc., UL 1278 Standard for Moveable and Wall or Ceiling Hung Electric Room Heaters, September 14, 2017.

G. There is a Critical Need for Enhanced CPSC Staff Expertise, Experience and Skills in the Areas of IoT and Other Emerging Technologies

The number of variety types technologies being incorporated into consumer products is increasing. As a result, for the CPSC to effectively assess potential safety risks, there is a critical need for CPSC to secure staff with expertise, experience and skills in this area. As acknowledged by CSPC staff in the Emerging Technologies Report, currently there are some gaps in CPSC staff expertise, specifically when it comes to evaluating software in consumer products.[18] Software is a key component to allowing products to be connected to the internet and having CPSC expertise in this area is critical. RILA urges the CPSC to expand staff's knowledge base in this area to better understand IoT, AI and other emerging technologies and the capabilities of connected consumer products.[19]

The CPSC could also look to actions taken by industry for ways the agency can keep pace with new and emerging technology and innovations. Many companies have hired a Chief Technology Officer (CTO) or Chief Innovation Officer (CIO). CTOs and CIOs help companies navigate the rapidly changing landscape of new technologies, hardware, software, systems and products. A CTO/CIO could help the CPSC develop an action plans to address many of the issues outlined in the Emerging Technology Report, the IoT Hearing testimony and the comments in this proceeding. A CTO/CIO could monitor the marketplace and lead outreach to industry on where technology is being used in new consumer products. In addition, the CTO/CIO could be charged with managing a working group comprised of interested stakeholders, including CPSC commission and technical staff, dedicated to reviewing new technology and identifying potential product safety implications surrounding it.

In industry, a CTO's/CIO's responsibilities include helping a company determine and implement new technology the company needs to enhance customer experience and engagement, streamline operations and business processes to increase efficiency and effectiveness, and generate cost savings. Similarly, a CPSC CTO/CIO could help the agency identifying ways to use technology to increase and enhance the agency's public outreach and stakeholder engagement and streamline operations and work flows. Considering the CPSC's limited budget, having the CTO/CIO position fulfill several vital functions within the agency would conserve scarce budgetary resources. RILA encourages CPSC to consider hiring a CTO/CIO to fulfill a variety of functions within the agency.

III. Opportunities for the Retail Industry Collaborate with the CPSC to Promote Safety of IoT Products

Retailers have a unique perspective when it comes to IoT technology as companies are both users of the technology in retail operations and supply chains as well as sellers of IoT products to consumers. Retailers generally are not manufacturers of IoT products, and therefore, would not

[18] U.S. Consumer Product Safety Commission, *Potential Hazards Associated with Emerging Technologies*, 6, January 18, 2017.

[19] As mentioned in RILA's testimony of May 16, CPSC could consider reaching out to manufacturers, software developers, industry groups, retailers, the American Bar Association, Consumer Reports and other consumer advocacy groups for feedback on what products currently exist to gain insight into the current marketplace.

be able to share expertise with the CPSC on product design and development. However, retailers can provide "front line" feedback on connected products from consumers. Retailers are often the first point of contact for consumers when an issue arises with a product or a safety incident occurs. With new consumer products incorporating IoT and other new technologies entering the market daily, the CPSC desperately needs timely product specific incident information to be able to identify emerging product safety trends in this product category.

RILA's prior testimony and comments have highlighted the value of real-time product specific data that is provided to the CPSC as part of the retailer reporting program (RRP).[20] RILA has long urged the CPSC to formalize and expand the RRP into a formal government/industry partnership program with clearly defined rules and benefits for participation, including: 1) a partnership program report being accorded treatment as an "initial report" under Section 15b and 2) participation in the new government/industry partnership program qualifying as a mitigating factor in penalty and enforcement cases. The CPSC would benefit by obtaining real-time data on potential safety issues involving IoT and other consumer products, which would enable the agency to more quickly identify emerging risks and potential product safety trends and remove unsafe products from the marketplace. RILA continues to urge the CPSC to expand and formalize the RRP program so that critical information can be shared. In this era of breakneck paced change in IoT and technology enabled consumer products, a formal government/industry partnership program would be a major step forward in protecting the safety of consumers.

In addition to helping to drive new exciting and innovative consumer products, new technology developments are also radically changing the retail industry as customers use technology to shop, purchase and track delivery of products. In 2017, RILA launched its (R)Tech Center for Innovation ((R)Tech Center) to help members navigate the current disruptive change and transformation in the retail sector. The goal of the (R)Tech Center is to enable retail transformation and continued success by: connecting retail executives to innovative companies and technologies (e.g., IoT, AI, blockchain, augmented and virtual reality, robots, drones, etc.); fostering innovation through a newly launched (R)Tech Open Innovation Engine; building a talent pipeline promoting the retail industry as a technology-forward industry; and engaging in authoritative research. While the scope of the (R)Tech Center's work is not solely focused on IoT issues, because this technology is increasingly becoming a part of consumers' daily life and business operations, IoT issues will inevitably be encapsulated in the work done here. Through the work being done by the (R)Tech Center, we hope to be able to provide the CPSC with information and resources on this new and innovative technology in the future.

Conclusion

We thank the CPSC for the opportunity to testify and comment on the appropriate role of CPSC in ensuring the safety of consumer products that incorporate IoT and other emerging

[20] *See* Retail Industry Leaders Association, Comments on CPSC's Fiscal Year 2018 Priorities and 2019 Budget, 13 July 2017; *see also* Retail Industry Leaders Association, Comments on CPSC FY 2017 and 2018 Agenda and Priorities 6, 1 June 2016 and Retail Industry Leaders Association, Testimony on Data Sources and Consumer Product-Related Incident Information, 25 June 2015.

technologies. We look forward to working with the commissioners and staff on this critically important issue. Please do not hesitate to reach out to RILA for help on these efforts and any others the agency is considering. Feel free to contact me or Autumn Moore, RILA's director of regulatory affairs and compliance at autumn.moore@rila.org or 703.457.7919 if you have any questions.

Sincerely,

Kathleen McGuigan
Senior Vice President & Deputy General Counsel

Autumn Moore
Director Regulatory Affairs & Compliance