Status Report on the Internet of Things (IoT) and Consumer Product Safety

September 25, 2019

For further information, contact:

Patricia K. Adair

Office of Hazard Identification and Reduction

301-504-7335; padair@cpsc.gov

The views expressed in this report are those of the CPSC staff, and they have not been reviewed or approved by, and may not necessarily reflect the views of, the Commission.

1 Executive Summary

This report updates staff's progress on activities related to the Internet of Things (IoT), as specified in the Commission's fiscal year 2019 Operating Plan. The CPSC's mission is to protect consumers from unreasonable risk of injury from consumer products under its jurisdiction. The IoT is not a consumer product; instead, it is an enabling technology that allows connected products to bring new and innovative functionalities to products. The IoT allows consumers to affect physical change remotely in consumer products, offering unique opportunities to enhance consumer product safety, while simultaneously presenting new risks.

CPSC staff is working to gain an understanding of the best way to define consumer product safety in terms of the IoT, the intersection of, and interdependencies among consumer product safety, data security and privacy, and how our traditional risk management approaches apply to these products. Cybersecurity, privacy, and consumer product safety traditionally have been addressed independently by various federal agencies with jurisdiction in these areas. CPSC does not consider personal data protection and privacy to be consumer product hazards that we would address, absent an associated unreasonable risk of injury.

Following the Commission's 2018 public hearing on IoT and Consumer Product Safety, and learning from the comments submitted during and following the hearing, staff engaged in many activities to address the safety of Internet-connected products. Our work focused on three areas:

- Developing staff expertise and in-house capabilities for Internet-connected products (education/workforce development)
- Participating in and developing voluntary consensus standards (domestic and international)
- Collaborating with other federal agencies, foreign governments, and with a wide range of stakeholders.

Staff learned a great deal from government and industry experts and educated outside stakeholders about CPSC's niche in the current world of IoT-connected products. Our mission is simple: Keep consumers safe from unreasonable risks presented by consumer products. The IoT presents a unique intersection point that has the potential to change the CPSC's thinking about how to address product safety for connected products. For connected products, the concept of "unreasonable risk" shares a nexus with data security. A connected product could present an unreasonable risk of injury due to problems with its software updates or customization, its connection, or its data. Connected consumer products are, by their very nature, part of a digital environment, which means that data security risk management is part of consumer product safety.

TABLE OF CONTENTS

2 INTRODUCTION

On January 17, 2017, the CPSC published a staff report[1] that identified emerging technologies and trends expected to become available for use, or gain wider use, in the ensuing 3 to 5 years. The report identified new, increased, or decreased consumer hazards associated with these new technologies. Staff identified several technological and societal trends that are likely to influence the marketplace for consumer products. Prominent among the identified trends i increased integration of smart technologies and IoT. Recognizing that Internet-connected consumer products are a rapidly expanding trend, staff also researched new and potential consumer product technologies and the related consumer safety issues – as well as opportunities for enhancing product safety – that the Commission may want to consider in analyzing, prioritizing, and managing risk. In fiscal year (FY) 2019, staff focused efforts on understanding the safety implications of Internet-based smart technologies, software as a component of a consumer product, wearable technologies, and technologies that complement and enhance the functionality of products, including virtual reality and artificial intelligence (AI).

This report on IoT-related activities updates the Commission on staff's progress in accordance with the Commission's FY 2019 Operating Plan.[2] Staff is working to develop a best practices guide for connected consumer products as well as recommendations for practical ways consumers can mitigate their risk from the potential *hazardization*[3] of Internet-connected consumer products.

2.1 WHAT IS THE INTERNET OF THINGS?

The CPSC's mission is to protect consumers from unreasonable risk of injury associated with consumer products under its jurisdiction. The IoT is not a consumer product; it is an enabling technology to bring new and innovative functionalities to connected consumer products. The market for Internet-connected devices continues to expand, with about 64 billion IoT-connected devices expected to be available globally by 2025, a 6.4-fold increase from 2018.[4]

[1] U.S. Consumer Product Safety Commission Staff Report. Potential Hazards Associated with Emerging and Future Technologies. January 18, 2017. https://www.cpsc.gov/s3fs-public/Report%20on%20Emerging%20Consumer%20Products%20and%20Technologies_FINAL.pdf

[2] U.S. Consumer Product Safety Commission Fiscal Year 2019 Operating Plan. Approved October 10, 2018. Available at: https://www.cpsc.gov/s3fs-public/FY-2019-Op-Plan.pdf?ikxHwe_np9E_1b7iFHC.8i_yLBGq1dc5

[3] Hazardization is the process by which a product, which would otherwise be safe, poses a danger to consumers when connected to the Internet is subjected to unauthorized, imprudent, or anomalous data transfer interference or manipulation of operational code or consumer-originated data, with the potential to cause injury or death. This concept is more fully explored in section 2.4 of this report.

[4] Peter Newman, The Internet of Things 2019 Report: How the IoT Continues to Transform Business, Homes, and Cities Through Next Generation Digital Solutions, Bus. Insider Intelligence (January 2019). https://store.businessinsider.com/products/the-internet-of-things-report?IR=T&itm_source=businessinsider&itm_medium=content_marketing&itm_campaign=report_teaser&itm_content=full_report_text&itm_term=store_text_link-internet-of-things-report&vertical=iot#!/The-Internet-of-Things-Report/p/46301489

There is no globally accepted definition of the IoT. The Organization for Economic Co-Operation and Development (OECD) refers to IoT as "an ecosystem in which applications and services are driven by data collected from devices that sense and interface with the physical world".[5] The U.S. Government Accountability Office (GAO) describes the IoT this way:

> ". . . 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."[6]

In general terms, the IoT can be divided into Industrial IoT (business- or workplace-related) and Consumer IoT (consumer product-related). Our focus is on the Consumer IoT and the consumer products that are connected to the Internet or other network directly or indirectly, or *connected products*. To that end, staff is participating on a task group in an ASTM International (ASTM) activity to develop a standard guide for connected consumer products. The task group's current draft working definition of "connected products" states:

> 1.2 Connected Product means any device or physical object that is capable of connecting to the Internet or other network directly or indirectly, and that is assigned an Internet, a Bluetooth, or other communication protocol address or identifier. A non-exhaustive list of examples includes:
>
> a) connected children's toys and baby monitors;
> b) connected safety-relevant products such as smoke detectors and door locks;
> c) smart and/or security cameras, TVs and speakers;
> d) wearable health trackers and apparel;
> e) wearable smart apparel;
> f) connected home automation and alarm systems;
> g) connected appliances (*e.g.*, washing machines, refrigerators); and
> h) smart home assistants.

2.2 Jurisdiction

Data security,[7] privacy and consumer product safety have traditionally been addressed independently by various federal agencies with jurisdiction in these areas. The CPSC has not considered data security and privacy issues related to consumer products to be hazards we would address, absent an associated unreasonable risk of injury.[8]

[5] OECD. Consumer Product Safety in the Internet of Things, OECD Digital Economy Papers, March 2018.

[6] U.S. Government Accountability Office, GAO-17-570.

[7] Data security, as we use the term in this report, is a subset of cybersecurity. Data security is about improving the confidentiality, integrity, and availability of data, depending on the use-case needs and circumstances. Confidentiality is about the data staying secret, if needed. Integrity is confidence that the data has not been altered, purposefully or even in an unintended way (*e.g.*, a loss/error-prone network connection). Availability is confidence that the data will be there when needed and can be very important in certain use-cases (*e.g.*, medical). Cybersecurity concerns the security of data, but also the security of systems and their components (*e.g.*, devices). Beyond the three aspects described above, this would also concern aspects of systems, such as resiliency of the system in the face of attack through mitigations, such as patch and vulnerability management.

[8] 83 Fed. Reg. 13122; March 27, 2018.

Staff is working on how to define consumer product safety in terms of the IoT, the intersection of, and interdependencies among, consumer product safety, data security and privacy, and how our traditional risk management approaches apply to connected products. In the current world of IoT-connected consumer products, the concept of "unreasonable risk" shares a nexus with data security.

2.3 The IoT Presents Benefits and Challenges for Product Safety

Many connected consumer products offer safety benefits to consumers. Connected consumer products can provide alerts in situations that involve consumer safety. For example, electronic personal assistants and distributed sensors in the home can detect problems and notify consumers of safety issues through smartphone alerts and interconnected alarms. This enhancement could be a boon to the safety of the elderly, many of whom would like to remain in their own homes, or "age in place."

IoT-enabled traceability could help companies accurately identify problems, effectively notify consumers, remotely repair product defects, and proactively limit the scope of product recalls. Manufacturers could improve recall effectiveness if consumers can be notified directly of product recalls–especially through automatic product registration−and the remedy can be automatically pushed out to the affected products. With such potential advantages, however, come some potential drawbacks. For example, proper notice could in fact be curtailed if manufacturers or retailers simply corrected defective products via the Internet without notifying the public, affected individuals, or the CPSC.

Staff has several concerns with connected consumer products:

- *Addition of remote operation feature for products that could be hazardous if operated remotely*. For example, products such as gas grills and space heaters can pose potential fire and carbon monoxide hazards if turned on remotely;
- *Hazardization of a consumer product after purchase.* A consumer product that did not present an unreasonable risk of injury at the point of sale could become "hazardized" if unauthorized, imprudent, or anomalous data transfer interference or manipulation of operational code or consumer-originated data create a safety hazard where one did not exist before (*e.g.*, a connected gas range pushes a software update that disables temperature-limiting capability);
- *Disabling a safety feature.* Changes to a product's software, or to a device to which a product is connected, could lead to disabling a safety feature. For example, software updates to a connected home security system could inadvertently lead to disabling a smoke or carbon monoxide alarm without the homeowner's knowledge;
- *Clarity for consumers on critical data security and safety function support.* Consumers need clarity on when an IoT device might no longer be safe to use due to termination of software updates.

A connected product could present an unreasonable risk of injury due to problems with its software updates or customization, its connection, or its data. Connected consumer products are, by their very nature, part of a digital environment, which means that data security risk management is part of consumer product safety.

2.4 Hazardization

The transformational characteristic of IoT products having the greatest impact on product safety for the CPSC is the increased potential for unseen product *hazardization*. Hazardization occurs when a product becomes unsafe after purchase because it has changed. Product hazardization can happen due to:

- Malicious hacking
- Defective third party software
- Defective manufacturer updates
- Consumer modifications.

For non-connected products, hazardization typically occurs from tampering by unqualified persons or by consumers wishing to defeat an unwanted safety feature. It may also result from excessive and unreasonable abuse from mechanical, thermal, or electrical shock. Normal wear and tear can also create unsafe conditions in products still in use beyond the designer's intended end-of-useful life. Hazardization incidents, as described above, typically would not be surprising and may or may not be seen as defects.

For IoT products, the potential for unexpected hazardization flows directly from device connectivity and the invisibility of data processing. Consumers typically would not be aware that, after purchase, due to unauthorized, imprudent, or anomalous data transfer interference[9] or manipulation of operational code or consumer-originated data, an IoT product capable of causing injury or death had become hazardized. Examples include: the robotic vacuum that loses its way and falls down the stairs onto a small child due to a poorly designed third-party app or the connected heating system in the home of an elderly resident that shuts down on a bitterly cold winter day after the software is hacked. In such cases, a consumer could not anticipate the data security defect that allowed the change in the product and the resulting hazardous condition.

Another challenge presented by cyber defects in a world of mobile personal IoT devices involves injuries or deaths facilitated by, but not directly caused by, the connected device. An example of this would be a defective software update in a wearable GPS-enabled watch that, in error, leads a consumer to walk into a hazardous area and become injured in a fall.

As discussed above, hazardization of connected products will challenge product safety regulators to respond appropriately. Whether through direct government intervention, or via voluntary consensus standards, the physical safety of consumers in a connected world must be protected. For the CPSC, this effort requires understanding rapidly emerging technologies, how personal data are used by these technologies, and the security fundamentals necessary to keep consumers safe.

[9] Data transfer interference at the device, not within the public network.

2.5 Data Security

The protection of data and data processing systems is generally known as "cybersecurity." Cybersecurity practices aim to ensure the availability, integrity, and confidentiality of data in defined environments. Because confidentiality would not typically fall within the CPSC's mandate, we use "data security" to capture the elements of availability and integrity. In an IoT product, data security concerns all of the data stored in, or moving in or out of a connected device that could impact the safety of the product. This includes:

- Operational instructions (software)
- Consumer originated data (*e.g.*, biometrics, settings and preferences, multiple-user identification)
- Environmental metrics (*e.g.*, location, temperature, atmosphere, energy)
- Manufacturing/Product data (*e.g.*, serial numbers across products)

If a safe product becomes *hazardized* by modification or manipulation of its data, whether that is its software or data supplied by consumers, or through environmental metrics, the CPSC may have cause to identify the defect that permitted access to the data in question. Stated another way, the CPSC would be looking for a potential defect in data security that created an unreasonable risk of injury.

3 Federal Government Leadership on IoT

Although there is no national strategy for the IoT, in June 2017, the U.S. Department of Commerce (DOC) issued the report *International Cybersecurity Priorities: Fostering Cybersecurity Innovation Globally*,[10] in response to Presidential Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*.[11] The DOC report described priority areas and broadly categorized them into five overarching themes:

1. Encouraging and facilitating cybersecurity innovation through the global marketplace
2. Ensuring cybersecurity approaches and policies are globally relevant
3. Advocating for U.S. cybersecurity products and services internationally
4. Enhancing global Internet security and stability
5. Building international capacity on cybersecurity education and workforce.

Furthermore, the DOC report recommends that the U.S. government continue to:

- advocate internationally for industry-led and consensus-based cybersecurity standards and effective, voluntary solutions;

[10] https://www.commerce.gov/sites/default/files/2018-06/International%20Cybersecurity%20Priorities%20Report.pdf.

[11] https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/.

- advocate that intergovernmental organizations' outputs should not include prescriptive text calling for global cybersecurity legal frameworks or cybersecurity treaties, to ensure cybersecurity solutions remain flexible;
- focus on international adoption of cryptographic technologies;
- expand international participation in multi-stakeholder processes with international partners; and
- leverage cybersecurity educational initiatives to build capacity among key partners and show American leadership internationally.

Staff notes that despite the CPSC's product safety jurisdiction over the vast majority of connectable consumer products, there has been little recognition, to date, from Congress of CPSC's role in government-wide cybersecurity policy. We expect this to change as a result of CPSC's leadership role in establishing the interagency IoT working group and other staff engagement with key IoT policymakers.

4 Commission Activities on IoT

4.1 Public Hearing

On May 16, 2018, the Commission held a public hearing on the Internet of Things and Consumer Product Hazards. In the *Federal Register* Notice (FRN)[12] announcing the public hearing, the agency requested information from all interested parties about potential safety issues and hazards associated with Internet-connected consumer products, as well as benefits of this new technology to consumers. The same consumer hazards that are associated with traditional consumer products are also associated with IoT products, including fire, burn, shock, tripping and falling, lacerations, contusions, and chemical exposure. The FRN noted that CPSC did not consider personal data security and privacy to be consumer product hazards that the agency would address. Thirteen organizations provided testimony at the public hearing. Following the public hearing, the CPSC received written comments from a variety of stakeholders. The written comments are found at regulations.gov, docket no. CPSC-2018-0007.

Several general themes emerged from the public hearing testimony and written submissions (some of them conflicting), which are summarized below.

4.1.1 Certification/Third Party Testing

Some commenters opposed mandatory certification of connected products, while others supported mandatory certification and third party testing of high-risk products.[13] One commenter asserted that if CPSC were to require certification of connected products, then certification standards should be tailored to particular categories of products having similar functions or

[12] The Internet of Things and Consumer Product Hazards, Request for Comments, Docket No. CPSC-2018-0007. 83 Fed. Reg. 13122; Mar. 27, 2018. https://www.regulations.gov/docket?D=CPSC-2018-0007

[13] 83 Fed. Reg. 13122; Mar. 27, 2018. ("Should certification to appropriate standards be required before IoT devices are allowed in the marketplace?")

safety profiles. The commenter added that if CPSC relies on certification, the Commission should work to align with other existing national or international certification schemes and ensure there are adequate accreditation requirements.

Commenters, including the Federal Trade Commission (FTC), stated that the CPSC should consider requiring manufacturers to state publicly the standards to which they adhere. Such disclosures, the commenters maintained, would improve transparency and provide consumers with information to evaluate safety and security of IoT products better. The FTC stated that it could use its authority under the FTC Act to take action against companies that misrepresent their security practices in their certifications.

4.1.2 Consumer Education

Some commenters stated that CPSC should educate consumers on the importance of learning about connected products; encourage consumers to buy products that have strong security; and recommend that consumers download and install updates, and they suggested that CPSC work with industry stakeholders to educate consumers on IoT product risks through documentation (user manuals) and warnings. Additionally, a commenter suggested that CPSC share product safety insights with consumers in as many ways as possible, including creating a series of case studies on IoT-connected devices that have had safety issues so that consumers understand the potential risks.

4.1.3 CPSC IOT Standards Activities (voluntary standards and mandatory regulations)

The majority of commenters supported development of voluntary standards for connected products, noting this new technology is in its nascent stages and regulation could stifle innovation. Commenters encouraged increasing CPSC’s resources for voluntary standards development, including participation in international standards organizations, such as International Organization for Standardization (ISO) and International Electrotechnical Commission, as global alignment or harmonization is preferred.

Some commenters felt that process-based or “best-practice” guidance documents are likely to be more effective than performance standards. If regulations are developed for IoT devices, commenters suggested they be technology-neutral and sufficiently flexible to allow for changes in technology.

Commenters also noted that some existing voluntary standards and regulations may need to be updated to include specific requirements for Internet-connected controllers (*i.e.*, update the safety standard for garage doors to include tests for Internet-connected control systems).

One commenter noted that ASTM F963 *Standard Consumer Safety Specification for Toy Safety* addresses product safety hazards for children’s toys but does not identify physical hazards presented by an Internet-connected toy.

Some commenters advocated for regulation. Specifically, one commenter supported a “reasonableness standard” that would require that all manufacturers of connected products to possess proof of reasonably substantiated code safety for each product.

4.1.4 Existing Cybersecurity Frameworks and Best Practices

Many commenters suggested CPSC learn more about existing cybersecurity frameworks and guidance documents before developing guidance for consumer product safety. Several commenters suggested CPSC learn about the National Institute of Standards and Technology (NIST) Cybersecurity Framework and NIST security standards to the extent they can reduce the risk of product hazardization. Other commenters advised the agency to consider the Online Trust Alliance (OTA) IoT Trust Framework, which provides a set of principles for security of IoT devices and related services to protect consumers and the privacy of their data. OTA also has a Smart Home Checklist and Enterprise IoT Checklist that are designed to educate consumers and other users on the proper use of IoT-connected devices in specific contexts. These resources could be used or adapted for consumer safety initiatives.

Commenters suggested reviewing IoT voluntary guidance documents issued by other agencies, including the FTC, the National Highway Traffic Safety Administration (NHTSA), and the Food and Drug Administration (FDA).

4.1.5 Incident Data

Several commenters noted that CPSC’s incident reporting systems may need to be updated to capture IoT-related issues, and they offered suggestions for capturing connected products in our data systems, including an IoT designation in its National Electronic Injury Surveillance System (NEISS). Similarly, commenters suggested CPSC may want to consider adding an IoT designation on the form, “Report an Unsafe Product,” on saferproducts.gov.

Commenters noted there is value in CPSC identifying and openly sharing incident data resulting from IoT devices, as this would be helpful in developing and applying horizontal standards,[14] where appropriate.

4.1.6 International Engagement

Commenters supported expanding international collaboration and cooperation on IoT-related issues, including CPSC participation in OECD meetings. CPSC and other U.S. regulators should share information about, and align their approaches with, comparable international bodies, while maintaining its focus on how the IoT fits within existing U.S. law, according to commenters. Commenters emphasized harmonization of requirements, when appropriate, while respecting differences in national law and culture.

[14] A *horizontal standard* means a standard on fundamental principles, concepts, terminology or technical characteristics, relevant to a number of technical committees and of crucial importance to ensure the coherence of the corpus of standardization documents. This definition is from IEC Guide 108 *Guidelines for ensuring the coherency of IEC publications* ‐ *Application of horizontal standards*. Horizontal standards are typically developed where it is considered better to record a set of requirements in one place rather than to duplicate them in multiple requirements documents. This drives consistency in the relevant requirements, is more efficient (the horizontal standard is simply referenced), and it allows for the development of an expert group for the relevant subject matter.

4.1.7 Jurisdiction/Statutory Requirements

Several commenters stated that CPSC should stay within its jurisdictional and statutory authorities, noting that privacy and data security, as they have been understood, to date, are not within CPSC's jurisdiction. Addressing concerns over children's privacy, commenters noted that the privacy of children's information is covered by the Children's Online Privacy Protection Act[15] and enforced by the FTC. Other commenters maintained there is a lack of clarity regarding various federal agencies' jurisdiction.

4.1.8 Privacy, Data Security, and Product Safety

Several commenters noted that, while privacy and data security are not within CPSC's jurisdiction, connected products present new challenges for product safety. These commenters noted that the Commission should examine the intersection of privacy and security threats under existing laws.

Commenters noted "privacy and data security concerns are at the core of what consumers believe to be unsafe about IoT devices," adding that "failure of IoT software or a software update could potentially create safety risks for consumers." Discussing the need for strong security, a commenter noted that it is vital to restrict control and operation of devices, including authentication of users and code, secure communication, and the ability to update software or firmware, and they also emphasized the importance of well-tested products.

A commenter noted that when defining "hazardization" of connected products, CPSC should further consider the interplay between network connectivity, software, hardware, battery, data, and autonomous capabilities. Furthermore, a commenter stated that a potential product hazard enabled by connectivity is not simply a product hazard; it is a cybersecurity risk because it may provide a connected entry point through a vulnerable device to a vulnerable network. CPSC should pay attention to certain cybersecurity threats that create opportunities for physical harm, a risk not previously considered, and resist creating any prescriptive rules for IoT devices, the commenter noted.

A commenter encouraged the agency to consider the "failure" state of devices that lose connectivity or are interrupted during a software update. Devices like smoke alarms and thermostats should default to a working state that does not introduce a hazard risk and that should continue to function in their normal capacity.

Furthermore, one commenter stated that CPSC should develop a plan for addressing hazards associated with unsupported IoT devices and seek guidance from the National Telecommunications and Information Administration (NTIA), which runs a work group devoted to researching IoT security, patching, and upgradability. All IoT devices should be required to contain a "Bill of Materials," which could have a list of component materials, parts, and software used in the IoT device. A commenter encouraged CPSC to focus on Manufacturer Usage

[15] The Children's Online Privacy Protection Act of 1998 is a U.S. federal law, located at 15 U.S.C. §§ 6501–6506. The act, effective April 21, 2000, applies to the online collection of personal information by persons or entities under U.S. jurisdiction about children under 13 years of age.

Description (MUD) standards to address product safety issues that arise from malware or malicious code.

Other commenters stated the CPSC should focus on product safety, rather than broader cybersecurity risks. One commenter maintained that market forces will address many of the security concerns of IoT devices, as consumers will avoid products with poor security.

4.1.9 Staff Education/Workforce Development

Commenters noted that CPSC staff needs to develop expertise in IoT, through work with stakeholders, the international community, and other agencies, before CPSC issues guidance or initiates a regulatory activity. One commenter suggested that the agency hire a Chief Innovation Officer or a Chief Technology Officer to focus on IoT and other emerging hazards.

4.1.10 Recall Effectiveness

Several commenters discussed the benefits of connected products for CPSC, consumers, and manufacturers, particularly for improving recall effectiveness and supply chain management. Commenters noted that the IoT provides pathways for prompt notification to consumers of potential product safety issues, as well as the ability for manufacturers to identify and remedy safety risks at all stages of the product supply chain.

Commenters noted that connectedness and autonomy may promote automatic product registration and improve product traceability throughout complex global supply chains, reduce costs, maximize recall effectiveness, and enable manufacturers, distributors, and retailers to identify and remediate defective products before and after point of sale. One commenter said that CPSC should ensure that companies do not issue recall notices every time they patch security bugs.

4.1.11 Risk Assessment

Following the theme of collaboration, a commenter encouraged CPSC to work with other agencies to establish protocols for interagency collaboration on risk assessment and enforcement related to IoT products. Another comment encouraged the use of well-recognized product safety hazard analysis and risk assessment tools to manage potential product safety risks presented by IoT products.

4.1.12 Stakeholder Engagement

Commenters encouraged stakeholder engagement and had specific suggestions, including engaging with the NIST National Cybersecurity Center of Excellence (NCCoE) to develop best practices/process-based guidance, using the NIST Cybersecurity Framework; participating in the NTIA multi-stakeholder process; and generally supporting collaboration with industry and consumer stakeholders other federal agencies and international regulatory bodies.

4.2 Commissioner Kaye's IoT Framework Document

On January 31, 2019, the Office of Commissioner Elliot Kaye released a paper titled, "A Framework of Safety for the Internet of Things: Considerations for Consumer Product Safety."[16] In his accompanying statement Commissioner Kaye described the document as a compilation of considerations for designing safer connected products.

5 Staff Activities on IoT

The Commission's 2018 public hearing and the written comments that followed provided valuable information and excellent suggestions for addressing the safety of connected products. In FY 2019, staff formed an IoT Team to devise an interdisciplinary approach to the challenges and opportunities presented by connected products. Staff is taking a three-pronged approach to address the safety of Internet-connected consumer products. Our approach aligns well with the priorities and recommendations set out in the 2017 Department of Commerce report, as adapted to CPSC's mission:

- Developing staff expertise and in-house capabilities for Internet-connected products (education/workforce development);
- Participating in and developing voluntary consensus standards (domestic and international);
- Collaborating with other federal agencies, foreign governments, and with a wide range of stakeholders.

5.1 Developing Staff Expertise/Workforce Development

5.1.1 Interagency Agreement with NIST NCCoE

From discussions following the initial meeting of the CPSC-led Interagency WG, staff worked with NIST NCCoE to develop an Interagency Agreement to assist in developing staff expertise for testing connected products at the CPSC's National Product Testing and Evaluation Center (NPTEC). This agreement includes training on the use of NIST SPECIAL PUBLICATION 1800-15, *Securing Small-Business and Home Internet of Things (IoT) Devices: Mitigating Network-Based Attacks Using Manufacturer Usage Description (MUD)*, as it relates to ensuring safe consumer products. CPSC funds this project, which is a CPSC-NCCoE collaboration.

5.1.2 Development and Set-Up of IoT Testing Capabilities at the National Product Testing and Evaluation Center (NPTEC)

Staff is working to establish capabilities to simulate a home network connection, while independently maintaining the security of the CPSC corporate networks. This capability will allow technical staff to simulate a home network and accurately evaluate consumer products for potential hazards. Set-up of the IoT testing capabilities is expected to be completed by the end of

[16] Available at: https://www.cpsc.gov/s3fs-public/A_Framework_for_Safety_Across_the_Internet_of_Things_1-31-2019_0.pdf?1KJ.t4Tn04v9OtEBr2s0wyLAP.KsuuQ3.

2019, pending network security reviews, equipment set-up, and staff training on network access and control protocols to ensure overall network security.

This work will allow staff to develop a deeper knowledge of cybersecurity and connected consumer products, which is aligned with the DOC's recommendation to: *leverage cybersecurity educational initiatives to build capacity among key partners and show American leadership internationally*.

5.1.3 Staff Project Work on IoT

Beginning in FY 2019, and continuing into FY 2020, staff is executing three IoT projects summarized below.

1) *Developing and Executing a Methodology for Assessing Safety Performance Changes Related to Firmware Revisions in Microprocessor-Controlled Consumer Products*

The proliferation of the use of microprocessor controls in a wide range of consumer product categories from toys to propane grills, coupled with the ability of these products to connect to the Internet, enables manufacturers to update software, as necessary, fixing software bugs and glitches, or improving performance over the life of the product. Although this capability can be of great benefit to the user experience, or even help to improve the safe operation of a product, CPSC staff is aware of instances in which a software update has created an unintended condition from a confluence of several factors that result in safety risk. Staff is seeking the services of a contractor with expertise in software programming and hardware integration to develop and execute a methodology for testing and evaluating connected products.

To develop this methodology, under an initial task order, staff has identified two candidate case studies involving shared e-scooters.

2) *Remote Configurable Heating Appliance Assessment*

This project will analyze hazards exhibited by new "smart," network-connected heating appliances. The new network features allow for greatly expanded functionality, and with it, complex new patterns of use. Although connectivity can be used to increase consumer safety, the variety of new use-scenarios makes it difficult for manufacturers or the CPSC to determine whether consumers are being protected from the hazards inherent in heating appliances. The project will identify how these products can be used, methods of use promoted (by the manufacturers and outside parties), and the potential hazards arising from these new use-scenarios.

3) *Research on Smart Toys*

Technology has been transforming toys in many ways since CPSC issued the Age Determination Guidelines in 2002. Changes include increased interactivity with the user, declining cost of electrical components, more detailed die-cast molds and 3D printed prototypes, and increased presence of mobile devices/apps, which enable augmented reality and hybrid play with toys and books. The project involves examining a wide range of toys on the market with robotic and social media features in an effort to identify physical safety hazards.

5.2 Voluntary Consensus Standards Development

Staff actively participates in the development of consumer product consensus-based standards, and voluntary standards for connected consumer products are no exception. Voluntary consensus standards are generally easier than regulatory actions to revise in order to keep pace with new and emerging technologies.

Staff is working with ASTM International on a new voluntary standard guide for connected consumer products (*Standard Guide for Ensuring the Safety of Connected Products - Draft initiated)*. Additionally, staff is participating in Underwriters Laboratories Inc. (UL's) Cybersecurity Assurance Program (UL CAP), which uses the UL 2900 series for *Software Cybersecurity for Network-Connectable Products* and UL 5500 for *Remote Software Updates*. Both UL programs apply to certified Internet-connected products. These horizontal standards eventually are likely to be included in electrical product specific standards.

Staff continues to participate in voluntary standards development of related technologies, including emerging areas, such as wearable technologies, connected cooking systems, and artificial intelligence.

On May 30, 2019, staff participated in a NIST workshop to engage private- and public-sector organizations in discussions on federal engagement in the development of standards for Artificial Intelligence (AI).[17] Recognizing the need to develop expertise in this emerging area, staff enrolled in a 6-week online course on AI at the Massachusetts Institute of Technology.

This aligns with the Department of Commerce's recommendation to: *advocate internationally for industry-led and consensus-based cybersecurity standards and effective, voluntary solutions.*

5.3 Collaborations with Federal Agencies

5.3.1 CPSC's Interagency Working Group

In FY 2019, staff organized and led an Interagency Working Group (WG) on Consumer Product Safety of Internet-Connected Products. Participating agencies included the NIST NCCoE, the FDA, the FTC, the Federal Communications Commission, the Department of Energy, and the Department of Homeland Security. Additional agencies have expressed interest in joining the WG and will be invited to the next meeting to be held during the first quarter of FY 2020.

The WG serves as a focal point for information-sharing, research, and enforcement activities specific to Internet-connected consumer products. The purpose of the WG is to articulate and understand each agency's roles and responsibilities on Internet-connected products, identify potential gaps that agencies are experiencing, find opportunities to learn from each other in a collaborative manner, create an opportunity for interagency cooperation, promote the development of voluntary, consensus-based standards, and allow CPSC to develop high-level best practices guidance to ensure that connected consumer products are designed and produced to be safe and secure.

[17] https://www.nist.gov/topics/artificial-intelligence.

The WG met twice during FY 2019. The first meeting included a discussion on each agency's jurisdiction regarding connected devices and a presentation on NIST's Cybersecurity for IoT Program. The WG was briefed on the work of the ISO Technical Committee on Information Security. The second meeting included a presentation from Health Canada on the Canadian government's approach to the IoT and consumer product safety and discussion on work going on within the European Union and the OECD.

5.3.2 Coordination with NIST's NCCoE

The National Cybersecurity Center of Excellence, a group within NIST, is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address industries' most pressing cybersecurity issues.

Recognizing that NCCoE staff are the federal government's experts in the area of cybersecurity, CPSC staff is working with them to examine existing NIST cybersecurity frameworks and related documents to evaluate how we might customize and implement them to address consumer product safety issues. All of the NCCoE's documents are developed in an open, multi-stakeholder consensus process. In particular, staff is interested in NIST's draft "core capabilities" baseline[18] for connected products, as this list of considerations may be useful for staff's development of a draft best practices guidance document.

This aligns with the Department of Commerce's recommendation to: *advocate internationally for industry-led and consensus-based cybersecurity standards and effective, voluntary solutions.*

5.4 Collaborations with Foreign Governments

The CPSC participates actively in the OECD Working Party (WP) on Consumer Product Safety. The WP serves as a forum for sharing best practices among product safety authorities and for developing tools to assist governments and other stakeholders in their pursuit of safer products, for coordination, and policy alignment. The Global Recalls Portal[19] is one example of multilateral coordination, where recall information submitted by governments around the world are listed at a single OECD website.

The WP has recognized an urgent need for governments to discuss emerging and anticipated policies aimed at ensuring effective cybersecurity for connected consumer products. To inform such discussion, the WP has circulated a questionnaire to collect information about current and anticipated IoT cybersecurity policies. If, and when, governments move to mandate required levels of cybersecurity for connected products, it will be useful to know whether those mandates emerge as a disconnected array of requirements, specifically aligned with the individual missions of existing (or newly created) government agencies.

Staff hopes that the WP's initiative in the IoT space will be useful to governments and their constituent agencies as they work toward effective and cohesive IoT policies. NIST has joined

[18] NISTIR 8228 Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks. June 2019. National Institute of Standards and Technology, U.S. Department of Commerce. https://doi.org/10.6028/NIST.IR.8228

[19] https://globalrecalls.oecd.org/#/

CPSC staff in the early discussions in this effort at OECD, and we will continue to seek NIST's input to this forum as the technical agency with the best view of the U.S. government's own IoT policies.

In addition to participation in the WP, staff has also engaged colleagues working on IoT product safety in jurisdictions where we have traditionally had strong bilateral relationships, including Canada, the United Kingdom, and the European Commission.

This effort aligns with the DOC's recommendation to: *expand international participation in multi-stakeholder processes with international partners.*

5.5 Collaborations with Other Stakeholders

Staff traveled to conferences, participated in workshops and on panels, and met with stakeholders about the safety of Internet-connected products and CPSC's work, to date. Recent examples include:

- IoT World Conference, San Jose, CA
- WEAR 2019 Conference, Seattle, WA
- NIST Federal Engagement on AI Standards Workshop, Gaithersburg, MD
- Wearable Technology Conference and Expo, Santa Clara, CA
- UL Annual Meeting, Consumer Advisory Council IoT Panel Discussion, Wheeling, IL
- NIST Core Capabilities Workshop, IoT Panel Discussion, Gaithersburg, MD
- Consumer Federation of America Consumer Assembly, IoT Panel, Washington, DC
- ASTM Smart Textiles Workshop, Smart Textiles Regulators Panel, Denver, CO
- 2019 Consumer Product Safety Professional Certification Webinar Series (St. Louis University), *Wearable Products: A Case Study In Enhancing Your Safety Culture With Best Practices For Assessing Risks Associated With Emerging Technology Products*
- American Bar Association IoT National Institute Conference, Washington, DC
- NIST Workshop on Human Factors in Smart Technologies, Gaithersburg, MD
- NTIA Multi-Stakeholder meetings, Washington, DC
- IPC E-Textiles Workshop and Standards Meeting, Philadelphia, PA
- FTC's Regulators Cybersecurity Forum, Washington, DC

Staff's planned attendance at the 2019 Consumer Electronics Show (CES) in Las Vegas, NV, was canceled, due to the partial government shutdown.

5.6 Data Collection and Incident Reporting

Staff recognizes that our data collection techniques should be enhanced to capture information on issues with connected consumer products. The CPSC Integrated Product Teams are adding keywords to capture incidents involving connected products reported in CPSC 360. Staff has seen very few incidents, to date; but with the rapid proliferation of connected products entering the market, we expect to see an increasing number of incidents reported through our data systems.

Staff conducted internal training and worked within the offices of Hazard Identification and Reduction and Compliance and Field Operations to educate staff on recognizing Internet-connected products involved in incidents. In May, EXHR staff briefed the Field Supervisors on CPSC's IoT work, to date, and discussed the need to update the assignment messaging for connected products to obtain incident data. Specifically, staff proposed and drafted guidance documents to be used by field staff when investigating consumer products with Internet-connected incidents and hazards.

5.7 Product Safety Assessments

Technical staff performs Product Safety Assessments (PSAs) on consumer products to support compliance investigations. The Office of Compliance and Field Operations (EXC) is starting to assign PSA requests for connected products. For example, electrical and mechanical engineering staff is currently evaluating shared e-scooters. An e-scooter is an electrically propelled scooter with a handlebar and a platform for the placement of both feet inline and includes two inline wheels used by a rider standing on the platform. A shared e-scooter is a scooter that is leased on a short-term basis to a consumer for a fee, generally using a smartphone application. A shared e-scooter is not owned by the consumer, but rather, is owned by a ride-sharing platform company, who is responsible for leasing and maintaining the scooters. The hazards under evaluation are:

- Software-related braking issues;
- Electronic braking that may be partially controlled by software; and
- Potential hazards associated with lithium batteries and cells (part of existing project initiatives).

Staff is assessing what requirements may be recommended for shared e-scooters, considering factors such as:

- the software used and its update schedule;
- The maximum speed capability;
- any safety markings; and
- other safety features, including requirements for Internet-connected products.

6 Existing Frameworks and other IoT Guidance Documents

Many organizations, including industry trade associations, foreign governments, and federal agencies, are developing, or have developed, IoT frameworks and guidance documents. ASTM is working on ongoing voluntary standards development of a standard guide for connected consumer products. As mentioned, CPSC staff is working closely with NIST to understand how NISTIR 8228 *Considerations for Managing the Internet of Things (IoT) Cybersecurity and Privacy Risks* may relate to CPSC's mission to protect the public from unreasonable risk of injury from consumer products. We met several times with the NIST NCCoE staff to discuss potential voluntary best practices, as NIST continues to work on potential "core capabilities" for connected devices.

As we continue to review cybersecurity frameworks, best practices, and guidance documents, we are identifying the commonalities among them. For example:

- Which voluntary best practices are common to most approaches?
- Are there existing voluntary standards or widely accepted industry protocols that manufacturers could use to implement best practices?
- Can we map potential best practices to voluntary standards and/or industry protocols?

This approach could help staff establish voluntary best practices as the "floor" or foundation for the safety of connected consumer products under our jurisdiction.

7 Intersection of Data Security and IoT Product Safety

Staff is working to define product safety in terms of connected devices; the overlaps and interdependencies between IoT product safety, data security and privacy; and how our current definitions, voluntary standards, and regulations can be applied to connected products, or if they need to change to address product safety in the IoT ecosystem better.

The IoT is a unique interface between physical products and the Internet, with the potential to change the way we think about addressing product safety on connected products. As more connected products are available to consumers, increasingly, safety concerns involve digital security risks. This concept is recognized by the OECD.[20]

8 FY 2020 Planning

Staff learned a great deal from the Commission's 2018 public hearing testimony and written comments following the hearing. Staff acted on many of the commenters' suggestions. As discussed in this report, we:

- increased participation in voluntary standards development for connected products;
- established collaborations with a variety of stakeholders, including federal agencies and foreign governments;
- formed an Interagency Working Group on the Internet of Things and Consumer Product Safety;
- established an interagency agreement with NIST NCCoE on IoT workforce education and staff development;

[20] OECD, Bureau Document B Concept Note on the Overlap of Digital Security and IoT Product Safety. 22 July 2019.

- worked with foreign governments to align approaches to product safety for connected devices;
- began setting up an IoT lab at NPTEC for testing connected products; and
- led internal training for our Field Supervisors, and began updating data-collection protocols.

All of these efforts will continue into FY 2020.

In addition to ongoing project work and collaborations, staff proposes in the FY 2020 Operating Plan to undertake multiple IoT activities for FY 2020, including:

- Continuing our focus on potential safety issues with Internet of Things (IoT)/connected products, by developing a Best Practices Guide for industry and consumers;
- Engaging in voluntary standards development activities for IoT products;
- Building out IoT testing facilities at the National Product Testing and Evaluation Center; and
- Acquiring subject matter expert assistance on methods for testing IoT products.