# REPORT

# Artificial Intelligence and Machine Learning

# In Consumer Products

*May 19, 2021*


**For further information, contact:**

Nevin J. Taylor

Chief Technologist

Office of Hazard Identification and Reduction

(301) 509-0264 email; ntaylor@cpsc.gov

# EXECUTIVE SUMMARY

This report provides background information on Artificial Intelligence and Machine Learning (AI/ML) and outlines a proposed framework to evaluate the safety of these technologies in consumer products. Given the Consumer Product Safety Commission's (*CPSC*) mission to protect consumers from unreasonable risk of injury from products, this report includes recommendations for a program that identifies and analyzes potential hazards associated with AI/ML in consumer products. Although AI/ML has been discussed since the 1950s, the growing accessibility to large data sets and the hardware and software required to gather and analyze those data have made the use of AI/ML in consumer products a reality.

CPSC made AI/ML a priority in the fiscal year 2021 Operating Plan due to the expanding role AI/ML plays in consumer products. The Plan addressed the importance of assessing and analyzing these technologies to ensure that the use of AI/ML does not result in unsafe products. To that end, CPSC staff recently held an AI/ML Forum to obtain a range of stakeholders' views and perspectives. The objective was to identify the potential hazards and safety opportunities related to the use of these technologies in consumer products. Testing laboratories, consensus standards bodies, industry representatives, consumer groups, and academia highlighted their concern for trustworthy AI/ML and the significant impact that these technologies can present to the consumer.[1]

This report outlines efforts underway and recommended future actions the CPSC can take to identify safety concerns with AI/ML technologies. It reviews CPSC's current capabilities and proposes a framework that outlines an approach to evaluate the safety of these capabilities in consumer products. The report includes recommendations for a program that provides an essential capability to screen for these technologies and determine whether they contribute to hazards that can potentially create unsafe conditions for the American consumer. Specific initiatives will be proposed for Commission approval as part of annual Operating Plans.

[1] CPSC Artificial Intelligence Forum *Federal Register* notice: *https://www.federalregister.gov/documents/2020/12/01/2020-26441/cpsc-artificial-intelligence-forum.*

## TABLE OF CONTENTS

# INTRODUCTION

Within the last few years, AI/ML has emerged as one of the fastest growing technologies influencing consumer products. Since its inception at Dartmouth in 1954, AI/ML has existed in relative obscurity until recently. With the proliferation of sensors to collect data in real time, connectivity to afford the free flow of information, increased computing power to accommodate complex algorithms, and expanding consumer appetites for and applications of these technologies, there is a growing demand for AI/ML in today's modern marketplace. Given AI/ML's continual evolution and myriad applications, no single standard definition exists. For this report, we use the definitions from the National Defense Authorization Act (NDAA) of 2021 (Public Law No: 116-283), which states that the term ''artificial intelligence'' means a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations or decisions influencing real or virtual environments. Artificial intelligence systems use machine- and human-based inputs to—

(A) perceive real and virtual environments;
(B) abstract such perceptions into models through analysis in an automated manner; and
(C) use model inference to formulate options for information or action.

The NDAA also states that the term ''machine learning'' means an application of artificial intelligence that is characterized by providing systems the ability to automatically learn and improve on the basis of data or experience, without being explicitly programmed.

Given the lack of a universal definition, it is also worth noting the National Institute of Standards and Technology's (NIST) description of AI and its example of how these capabilities are applied:

**DESCRIPTION**: AI technologies and systems are considered to comprise software and/or hardware that can learn to solve complex problems, make predictions or undertake tasks that require human-like sensing (such as vision, speech, and touch), perception, cognition, planning, learning, communication, or physical action. [2]

**DEMONSTRATION**: Examples are wide-ranging and expanding rapidly. They include, but are not limited to, AI assistants, computer vision systems, biomedical research, unmanned vehicle systems, advanced game-playing software, and facial recognition systems as well as application of AI in both Information Technology (IT) and Operational Technology (OT). [3]

Artificial intelligence can be described as technologies with "if/then/else" processes that use a

[2] https://www.nist.gov/system/files/documents/2019/08/10/ai_standards_fedengagement_plan_9aug2019.pdf

[3] https://www.nist.gov/system/files/documents/2019/08/10/ai_standards_fedengagement_plan_9aug2019.pdf

pre-established logical model that applies techniques such as linear regression, decision trees, or other methods to derive predictions based on the data provided. [4] AI/ML technologies may support consumers in the detection, prevention, and reaction to various hazards. However, staff is concerned there are hazards unique to AI/ML technologies, particularly when the technologies are responsible for safety applications. Identified concerns include system failures, dangerous interactions among the system, user, and environment, and the potential for system evolution as it adapts to data and over-the-air updates.

Consistent with the NDAA definition of "ML," we consider ML to apply an iterative approach to learn and improve through contextual and adaptive correlation. It is through this view of AI/ML that the CPSC will approach these technologies in the ongoing effort to protect the public from the unreasonable risk of harm. The staff will focus on the following organizational priorities as it endeavors to establishment an AI/ML program:

- ✓ *Conducting research on potential product hazards from AI/ML in consumer products;*
- ✓ *Identifying incidents where consumers are injured due to AI/ML in consumer products;*
- ✓ *Developing new or enhancing existing voluntary consensus standards with industry to address AI/ML safety hazards in consumer products;*
- ✓ *Informing and educating consumers on AI/ML safety hazards in consumer products through the media, state and local governments, private organizations, and by responding to consumer inquiries;*
- ✓ *Obtaining the recall of consumer products that pose a substantial product hazard and arranging for their repair, replacement, or a refund; and*
- ✓ *Issuing and enforcing mandatory standards to address consumer product safety hazards due to AI/ML in products.*

Currently, there are no statutes that direct or authorize CPSC to regulate AI/ML applications specifically. However, the Consumer Product Safety Act and other statutes enforced by the Commission provide CPSC authority to regulate consumer products. (*See, e.g.*, 15 U.S.C. §§ 2051-2089). Therefore, consumer products with AI/ML integrated into them are within the agency's statutory authority.

At this stage, CPSC staff is working to address the safety concerns of potential hazards associated with these technologies by participating in the establishment and enhancement of voluntary consensus standards. As part of that effort, staff is developing a program to evaluate the potential safety impact of AI/ML throughout the design, development, and deployment lifecycle

[4] What to Expect from AI (MIT Sloan Management Review: https://sloanreview.mit.edu/article/what-to-expect-from-artificial-intelligence/

of consumer products that use these technologies. To that end, CPSC staff proposes a framework that includes, among others, the following questions:

- ***Do products have AI/ML components?***
  - *Screen for AI/ML components.*
- ***What are their functional features?***
  - *Assess the AI/ML capabilities.*
- ***How does it impact consumers?***
  - *Analyze foreseeable interactions and potential consequences.*
- ***When AI/ML learns is the next iteration still safe and reliable?***
  - *Ascertain if, and to what extent, the AI/ML technology transforms the product and/or its use over time.*

# FEDERAL AI/ML COORDINATION

The National Security Commission on Artificial Intelligence (NSCAI) Final Report identified what a profound impact AI will have on the economy, national security, and the welfare of our country. Thus, the NSCAI recommends a national approach. They noted that AI has the potential to influence society in a dramatic way. The report identified safety and reliability as a priority area for coordination of international technical standards. [5]

Executive Order 13859, "*Maintaining American Leadership in Artificial Intelligence,*"[6] requires the Director of the Office of Management and Budget (OMB), in coordination with the Director of the Office of Science and Technology Policy (OSTP), the Director of the Domestic Policy Council (DPC), and the Director of the National Economic Council (NEC), to issue a memorandum that provides guidance for the application of AI technologies to all federal agencies. The results are outlined in OMB M-21-06.[7] Recently, OMB released "Guidance for Regulation of Artificial Intelligence Applications,"[8] which informs the development of regulatory and non-regulatory approaches regarding technology and industrial sector AI capabilities. The guidance addresses the need to consider ways to reduce barriers to the development and adoption of AI technologies, and it calls for agencies to address their actions and identify current efforts underway in AI in five categories:

[5] The National Security Commission on Artificial Intelligence: *https://www.nscai.gov/*
[6] Maintaining American Leadership in AI: https://www.federalregister.gov/documents/2019/02/14/2019-02544/maintaining-american-leadership-in-artificial-intelligence
[7] Guidance for Regulation of AI Applications OMB M-21-06: https://www.whitehouse.gov/wp-content/uploads/2020/11/M-21-06.pdf
[8] Guidance for Regulation of AI Applications OMB M-21-06: https://www.whitehouse.gov/wp-content/uploads/2020/11/M-21-06.pdf

1. Statutory Authorities Directing or Authorizing Agency Regulation of AI Applications
2. Active Collections of AI-Related Information
3. AI Use Case Priorities
4. AI Regulatory Barriers
5. Planned Regulatory Actions Concerning AI Applications.[9]

NIST recently established an Interagency Committee on Standards Policy (ICSP) Artificial Intelligence Standards Committee Working Group (AISCWG) to facilitate government agency activities related to the development and use of AI standards. It is establishing a charter to develop recommendations relating to the definition, application, and standards for AI/ML. The overarching objective of this ICSP is to promote consistent federal policies, raise awareness, and foster effective coordination among federal agencies. Coordinating a collaborative approach will be an essential step in creating a consistent means of modeling and measuring AI/ML. This approach will afford AISCWG the opportunity to develop voluntary standards to analyze the potential for hazards that harm consumers.

# CPSC STAFF ACTIVITY

The CPSC hired a Chief Technologist (CT) with a background in AI/ML to address AI/ML product safety hazards. The CT established a cross-sectional CPSC AI/ML Working Group (WG). This team consists of CPSC staff with interdisciplinary expertise and experience throughout the organization. The WG is designed to develop capabilities and identify and address AI/ML consumer product safety hazards.

CPSC staff held a virtual AI/ML Forum on March 2, 2021, attended by more than 200 stakeholders. The forum included more than one dozen presentations and four panels, including presentations from the White House Office of Science and Technology Policy (OSTP), and NIST. The overall theme of the forum, as identified by consumer advocates, testing groups, and academia, referred to the evolutionary and transformational effect of this technology on consumers. Staff learned a great deal from the panelists, who highlighted current policies, principles, and standards, as outlined below:

1. *"Advancing Trustworthy AI," from the White House OSTP, focused on national level policy, principles, and initiatives.*[10]
2. *"Trustworthy and Responsible AI," from NIST, provided standards frameworks and highlights from the recently published NSCAI Final Report.*

[9] OMB M-21-06; Guidance for Regulation of Artificial Intelligence Applications: *https://www.whitehouse.gov/wp-content/uploads/2020/11/M-21-06.pdf*

[10] U.S. Leadership in AI: A plan for Federal Engagement in Developing Technical Standards and Related Tools: https://www.nist.gov/system/files/documents/2019/08/10/ai_standards_fedengagement_plan_9aug2019.pdf

Additionally, there were four AI/ML panels: *Policy, Standards, Program, and Consumer Safety.*

1. *The Policy panel consisted of presentations from the European Commission, the University of Nevada Las Vegas William S. Boyd School of Law, and Pennsylvania State University Law School, Engineering Department, School of Electrical Engineering and Computer Science. The presenters focused on policy considerations regarding AI/ML in consumer products.*
2. *The Standards panel included Underwriters Laboratories (UL), American National Standards Institute (ANSI), and the Consumer Technology Association (CTA) with presentations on Traditional Safety Standards, ISO JTC 1/SC 42 AI standard, and AI in Consumer Products.*
3. *The Program panel discussed a proposed framework for CPSC to address AI/ML in consumer products with presentations from Worchester Polytech Institute (WPI), American Council for Technology-Industry Advisory Council (ACT-IAC), UL, and the National AI Institute (NAII). The presenters identified AI/ML components and discussed implications of AI/ML capabilities, the impacts of AI/ML for consumer products, and concerns about the iterative and adaptive nature of AI/ML technologies.*
4. *The Consumer Safety panel discussed safety concerns and opportunities relative to AI/ML in consumer products from Kids in Danger, UL, Harvard, Testing Inspections and Certification, and Bureau Veritas. The panel addressed how to characterize products that are not static in nature. They provided examples where products changed in response to consumer inputs and interaction over time. The panel identified that these changes over time present challenges associated with evaluating products with AI/ML after an incident.*

The day concluded with a roundtable conversation regarding safety considerations surrounding the design, development, and deployment of AI/ML in consumer products. Informed by the forum, staff is developing an approach to:

- ✓ *Screen products for AI/ML components*
- ✓ *Assess the functions and features of their AI/ML capabilities*
- ✓ *Analyze potential hazards for safety considerations*
- ✓ *Monitor/measure product transformation to pre-established parameters.*

Staff examined how to operationalize the first step of the framework, as mentioned earlier, to determine how to integrate it into an actual program. Through a collaboration with CPSC staff, WPI students and professors, via WPI's Interactive Qualifying Project (IQP), developed methods to identify AI/ML components essential to creating AI/ML capabilities. These were the formative first steps to establishing a screening program. WPI's students produced a white paper that

outlines the methodology to screen products for AI/ML in sufficient detail to distinguish if products are AI/ML capable. In this white paper, WPI identified data sources, algorithms, computations, and connections as the components essential to produce an AI capability. Therefore, they postulated that a system is AI-capable if all four of these components are present.

Likewise, WPI found the components that define ML capabilities are: assessing and monitoring outputs, analyzing and modeling changes, and adjusting and adapting behavior over time. Applications of these AI/ML technologies may solve problems and/or develop evolving capabilities to adapt to the consumer and/or environment. These technologies may serve as a function of the product, like in the case of natural language processing (NLP), where AI/ML are incorporated into an extensive system to support effective and efficient operation. AI/ML also may take the form of a feature in some products, to assist the primary function to operate more effectively, or in some cases, ensure safe operations. In either capacity, each component is assembled to support or serve the entire AI/ML capable system.

The next step to address potential AI/ML safety hazards in consumer products is determining the function of the AI/ML capabilities. AI technologies process if/then/else logic models to take actions based on observations that inform decisions. Therefore, staff will need to understand the applications and their design and implementation to know when the AI/ML may be operating unsafely or leading to unsafe conditions or product settings.[11] As such, staff will need to address AI/ML product safety hazards by developing the means to assess and analyze the impact of these logical frameworks and empirical models.

By evaluating the components of AI/ML to characterize their potential capabilities, we can learn the direct cause, and resulting consequences, of the specific AI/ML application. This will require understanding not only the nature of the AI/ML, but also how it is implemented in the particular product under consideration. With this understanding, combined with how the consumer might use the product, and in what context and conditions, the impact of these AI/ML capabilities on safety can be identified and subsequent risk characterized. This process will provide CPSC staff the opportunity to characterize qualitatively and quantitatively the effects of AI/ML capabilities on safety in consumer products.

To that end, it may be possible to adapt tools developed for guiding security and privacy practices to create minimum safety standards. By exploring best practices for AI/ML and lessons learned throughout the design, development, and deployment of products, we can capitalize on other efforts to ascertain the level of safety in AI/ML products.

[11] What to Expect from AI (MIT Sloan Management Review: https://sloanreview.mit.edu/article/what-to-expect-from-artificial-intelligence/

# RECOMMENDATIONS

Given the rapidly evolving nature of AI/ML, and CPSC's nascent capabilities in this regard, collaboration will be key moving forward. Staff will seek to build upon the discussions at the AI Forum across a range of topics. Consistent with CPSC's approach in other product areas, a key collaboration focus is on voluntary standards development. Ongoing efforts can be leveraged to build upon a foundation of a growing body of work in this area including:

- ✓ *CTA 2089 R13 Definitions and Characteristics of AI*
- ✓ *CTA 2088.2 R14 Baseline Cybersecurity for Private Consumer Robotics*
- ✓ *ISO/IEC JTC 1/SC 2/WG 2 Universal Multiple-Octet Coded Character Set*
- ✓ *UL 2900 Standard for Software Cybersecurity for Network-Connectable Products*
- ✓ *UL 3300 Outline of Investigation Helps Advance Safety of Consumer, Service, and Education Robots*
- ✓ *UL 4600 Standard for Safety for the Evaluation of Autonomous Products*
- ✓ *UL 5500 Standard for Safety Remote Software Updates*
- ✓ *UL 8400 Standard to address safety for AR/VR/MR devices.*

In addition, staff will continue to leverage long-standing partnerships with the federal government, industry, and academia that have produced many key insights as to how to design, develop, and deploy AI/ML capabilities. Recent publications from these public-private partnerships help to provide common understanding of the technologies below:

- ✓ A primer on AI/ML,[12]
- ✓ A playbook to describe how to operationalize these technologies,[13]
- ✓ Standards for consistent means to monitor and measure AI/ML,[14]
- ✓ A framework evaluating AI/ML Bias, Fairness, Transparency, Responsibility, and Interpretability, as illustrated in the Ethical Application of AI tool (EAAI).[15]

Given these efforts, staff will recommend in the FY 2022 Operating Plan to continue active participation in AI/ML and to explore opportunities to develop voluntary consensus standards. In addition to voluntary standards work, gaps in product testing and evaluation capabilities need

[12] Artificial Intelligence / Machine Learning Primer: https://www.actiac.org/system/files/Artificial%20Intelligence%20Machine%20Learning%20Primer.pdf
[13] AI Playbook for the U.S. Federal Government: https://www.actiac.org/system/files/AI%20Playbook_1.pdf
[14] ACT-IAC Emerging Technology Community of Interest Response to NIST RFI on Artificial Intelligence: https://www.nist.gov/system/files/documents/2019/06/11/nist-ai-rfi-gsa_001.pdf
[15] Ethical Application of Artificial Intelligence Framework: https://www.actiac.org/system/files/Ethical%20Application%20of%20AI%20Framework_0.pdf

to be addressed. Although this can and will build upon previous work with contract support to develop software test and evaluation processes, undoubtedly, AI/ML will bring new and complex challenges. In particular, the continual transformation and perpetual evolution of these technologies will present unique challenges, given the resulting complexity to replicate incidents consistently.

To address these test and evaluation challenges, staff continues to explore collaborative efforts through stakeholder engagements. Included in these efforts is a planned proposal in the upcoming FY 2022 Operating Plan to explore an Interagency Agreement with the NIST National Cybersecurity Center of Excellence (NCCoE), leveraging Cooperative Research and Development Agreements (CRADAs) from various projects like Adversarial Machine Learning. Past workshops offered by NIST include[16]:

- ✓ *Exploring AI Trustworthiness – August 6, 2020*
- ✓ *Bias in AI – August 18, 2020*
- ✓ *Explainable AI Workshop – January 26, 2020.*

It is through engagements such as this that CPSC can develop staff expertise for testing AI/ML products. The knowledge gained and resulting experiences, complemented by potential future AI/ML workshops, will also aid in the development of standards to monitor and measure AI/ML capabilities. With the overlap of CPSC efforts on the Internet of Things (IoT), staff anticipates leveraging those capabilities. In its initial state, staff work will require ongoing collaboration among the AI/ML Working Group, investigators, data scientists, and AI/ML subject matter experts with the intent to support more independent work over time.

Ultimately, CPSC staff proposes to develop the means to screen for and identify AI/ML-capable products and seeks to develop checklists and tools for investigators and data scientists to collaborate with stakeholders. While this approach seeks to leverage existing CPSC technical capabilities and those held by other stakeholders, it is anticipated that shortfalls in the number of technical staff with software, and particularly, AI/ML expertise, will need to be addressed, given the projected growth in this area. Staff will develop a proposal for the Commission's consideration as part of upcoming budget and Operating Plan development.

[16] NIST AI Workshop Series: *https://www.nist.gov/artificial-intelligence/nist-ai-workshop-series*