April 29, 2022

Mr. Mark Przybocki
U.S. National Institute of Standards and Technology
100 Bureau Drive
Gaithersburg, Maryland 20899

RE: Comments of ACT | The App Association to the National Institute of Standards and Technology on its Artificial Intelligence Risk Management Framework Concept Paper

ACT | The App Association (App Association) appreciates the opportunity to submit views to the National Institute of Standards and Technology (NIST) on its initial draft of the Artificial Intelligence (AI) Risk Management Framework.[1]

The App Association represents thousands of small business software application development companies and technology firms that create the technologies that drive internet of things (IoT) use cases across consumer and enterprise contexts. Today, the value of the ecosystem the App Association represents – which we call the app economy – is approximately $1.3 trillion and is responsible for 5.7 million American jobs. Alongside the world's rapid embrace of mobile technology, our members create the innovative solutions that power IoT across modalities and segments of the economy. NIST's planned voluntary risk management framework (RMF)—and the efforts of numerous agencies with respect to AI policy and regulation—directly impact the app economy. We support NIST's goal of helping designers, developers, users, and evaluators of AI systems better manage risks across the AI lifecycle.

[1] https://www.nist.gov/system/files/documents/2022/03/17/AI-RMF-1stdraft.pdf.

1401 K Street NW Suite 501
Washington, DC 20005

202.331.2130 @ACTonline
ACTonline.org /actonline.org

The App Association also continues to work proactively to advance the integration of AI in key use cases. As just one example, the App Association's Connected Health Initiative[2] (CHI) assembled a Health AI Task Force in the summer of 2018 consisting of a range of innovators and thought leaders. CHI unveiled its AI Task Force's deliverables during a public-private multistakeholder dialogue in Washington, DC. These deliverables include a position piece supporting AI's role in healthcare, policy principles addressing how policy frameworks should approach the role of AI in healthcare, and a terminology document targeted at policymakers.[3] Since then, CHI has also developed Good Machine Learning Practices specifically for the development and risk management of AI meeting the Food and Drug Administration's definition of a medical device,[4] as well as recommendations on how to increase transparency for care teams and patients.[5] In general, the App Association continues to lead in advocating for the development of frameworks that will responsibly support the development, availability, and use of AI innovations.

AI is an evolving constellation of technologies that enable computers to simulate elements of human thinking – learning and reasoning among them. A broadly encompassing term, AI refers to a range of approaches and technologies, such as Machine Learning (ML) and deep learning, where an algorithm based on the way neurons and synapses in the brain change due to exposure to new inputs is used to develop a system capable of independent or assisted decision making.

AI-driven algorithmic decision tools and predictive analytics are having, and will continue to have, substantial direct and indirect effects on Americans. Some forms of AI are already in use to improve American consumers' lives today – for example, AI is used to detect financial and identity theft and to protect the communications networks upon which Americans rely against cybersecurity threats. Moving forward, across use cases and sectors, AI has incredible potential to improve American consumers' lives through faster and better-informed decision making, enabled by cutting-edge distributed cloud computing. As an example, healthcare treatments and patient outcomes stand poised to improve disease prevention and conditions, as well as efficiently and effectively treat diseases through automated analysis of x-rays and other medical imaging. AI will also play an essential role in self-driving vehicles and could drastically reduce roadway deaths and injuries. From a governance perspective, AI solutions will derive greater insights from infrastructure and support efficient budgeting decisions. An estimate states AI technological breakthroughs will represent a $126 billion market by 2025.[6]

---

[2] *See* www.connectedhi.com.

[3] The CHI's Health AI policy principles are available at https://actonline.org/2019/02/06/why-does-healthcare-need-ai-connected-health-initiative-aims-to-answer-why/.

[4] The CHI's Good Machine Learning Practices are available at https://bit.ly/3gcar1e.

[5] The CHI's health AI transparency recommendations are available at https://bit.ly/3n36WO5.

[6] McKinsey Global Institute, *Artificial Intelligence: The Next Digital Frontier?* (June 2017), *available at* https://www.mckinsey.com/~/media/McKinsey/Industries/Advanced%20Electronics/Our%20Insights/How

Today, Americans encounter AI in their lives incrementally through the improvements they have seen in computer-based services they use, typically in the form of streamlined processes, image analysis, and voice recognition (we urge consideration of these forms of AI as "narrow" AI). The App Association notes that this "narrow" AI already provides great societal benefit. For example, AI-driven software products and services revolutionized the ability of countless Americans with disabilities to achieve experiences in their lives far closer to the experiences of those without disabilities.

Nonetheless, AI also has the potential to raise a variety of unique considerations for policymakers. The App Association appreciates the efforts to develop a policy approach to AI that will bring its benefits to all, balanced with necessary safeguards to protect consumers. To assist NIST and other policymakers, the App Association has appended a comprehensive set of AI policy principles for consideration.[7] The App Association supports NIST's efforts to develop a voluntary prioritized, flexible, risk-based, outcome-focused, and cost-effective AI risk management framework (RMF), and strongly encourage NIST to align its voluntary RMF with these principles.

Noting our general support for NIST's efforts to develop a voluntary prioritized, flexible, risk-based, outcome-focused, and cost-effective AI RMF, we offer the following input on the initial draft of the AI RMF:

- The AI RMF initial draft appropriately covers and addresses AI risks, while maintaining a scalable approach to risk management, similar to the approach taken in NIST's Cybersecurity Framework. Such an approach recognizes that appropriate risk management practices reflect specific fact patterns and the unique risks posed by certain uses of AI. The initial draft of the AI RMF reflects that trustworthiness is sector-dependent and that particular risk management practices develop trust, and that risk management processes assist organizations to design and develop trustworthy solutions. We generally support NIST's proposed functions, categories, and subcategories that will assist organizations in using the NIST AI RMF once finalized.

  We also support the AI RMF initial draft's efforts to map to, and rely on, international standards such as from ISO-IEC/JTC-1-SC 42, IEEE, ASTM, and SAE. We recognize, however, that international standardization for AI risk management is not yet robust. As AI standardization matures, it will be important that NIST continue to update its AI RMF periodically (ideally annually), and that its collaborators abroad do the same.

%20artificial%20intelligence%20can%20deliver%20real%20value%20to%20companies/MGI-Artificial-Intelligence-Discussion-paper.ashx.

[7] *See* Appendix, *ACT | The App Association's Policy Principles for Artificial Intelligence* (outlining our organization's collective AI principles).

- We strongly support maintaining the initial draft of the AI RMF's reinforcement that it is voluntary, much like the NIST Cybersecurity Framework. NIST should recognize that some may attempt to position the NIST AI RMF as a mandatory standard of behavior (e.g., in litigation), and we encourage NIST's AI RMF to directly address this concern and reinforce in the NIST AI RMF that (1) adoption of the RMF is voluntary for the private sector and (2) that the RMF is not, and is not intended to be offered as, a baseline for behavior norms in the context of litigation.
- We again encourage NIST to ensure that the RMF prioritizes the design of AI systems, from the earliest phase of product development, being informed by real-world workflows, human-centered design and usability principles, and end-user needs. We recognize that this concept is reflected in the initial draft of the AI RMF, but to specifically encourage NIST to call on AI developers to build in AI quality through the data streams mentioned above "by design." AI systems solutions should facilitate a transition to changes in the delivery of goods and services that benefit consumers and businesses. The design, development, and success of AI should take advantage of collaboration and dialogue among users, AI technology developers, and other interested parties in order to have all perspectives reflected in AI solutions. As this concept must run across sectors and AI use cases, we call on NIST to advance thoughtful design principles in the RMF, and label them as such.

  We appreciate the initial draft of the AI RMF's design enabling the needs of different sectors and use cases to be addressed modularly. Different industries and sectors will need to focus on other impacted stakeholder groups due to, among other requirements, regulatory requirements (as a further example, the automobile industry may need to assess risks to the vehicle driver, to other drivers on the road, or to pedestrians), which underscores that the AI RMF must not impede different sectors' unique risk management needs.

  The required depth for risk analysis will also depend on established precedent. Using the healthcare sector as an example, for lower risk devices (e.g., a digital thermometer), showing the device is useable and useful to the intended user is sufficient; for higher risk devices (e.g., a pacemaker), manufacturers may be asked to show a more comprehensive risk/benefit analysis in the intended context of use, or a suitable clinical study. This is to say that, even within sectors, risk analysis will depend heavily upon the purpose the device serves—another indicator that different sectors will need flexibility in risk management processes.
- The success of AI depends on ethical development and use, which in turn impacts user trust and use of AI. The RMF should promote existing and emerging ethical norms for broader adherence by AI technologists, innovators, computer scientists, and those who use such systems. While ethical issues are

raised in the initial draft of the AI RMF, we call on NIST to include a new provision in its RMF providing for stakeholders' approaches to AI to duly consider ethics so that policies advance that:

- Ensure that AI solutions align with all relevant ethical obligations, across the lifecycle of algorithms or models.
- Encourage the development or updates of ethical guidelines to address issues emerging with the AI's use, as needed.
- Maintain consistency with international conventions on human rights.
- Ensure that AI is inclusive such that AI solutions beneficial to consumers are developed across socioeconomic, age, sex, gender, geographic origin, and other groupings.
- Reflect that AI tools may reveal extremely sensitive and private information about a user or group and ensure that laws protect such information from being used to discriminate against certain consumers.

- The App Association supports NIST's efforts in the initial draft of the AI RMF in helping providers, technology developers and vendors, and others involved to understand the distribution of risk and liability in building, testing, deploying, and even decommissioning AI tools. The RMF should advance the appropriate distribution and mitigation of AI-related risks and liabilities. That is, those in the value chain with the ability to minimize risks based on their knowledge and ability to mitigate should be incentivized take reasonable steps to do so. Further, the RMF should clearly state that those developing, offering, or testing AI systems provide truthful and easy to understand representations regarding intended use and risks that would be reasonably understood by those impacted (as well as expected to be impacted) to use the AI solution. References to "intended use" and "context of use" as concepts is an appropriate approach for AI risk management, which encourages AI developers to identify and model to address challenges prior to algorithm development, which in turn allows developers to identify and evaluate potential threats more effectively. A focus on intended use also discourages generating solutions first and fitting those solutions to a problem second, which increases risk that possible threats, such as bias, are overlooked. Developing this aspect of the AI RMF should include consulting with consumers, as well as developers of AI and other stakeholders.
- Building on NIST's longstanding leadership in supporting voluntary consensus standards, the App Association strongly encourages NIST to ensure that the AI RMF supports public-private collaboration on AI through standardization in standard-setting organizations (SSOs) (such as IEEE[8]). The RMF should support pro-innovation policies that encourage private sector research and development

[8] https://standards.ieee.org/initiatives/artificial-intelligence-systems/index.html.

of AI innovations and the development of related standards.

It is critical that the United States ensure that AI standards are accessible to innovators by promoting a balanced approach using those standards, including with respect to standard-essential patent (SEP) licensing. AI technical standards, built on contributions through an open and consensus-based process, bring immense value to consumers by promoting interoperability while enabling healthy competition between innovators; and often include patented technology. When an innovator gives its patented technology to a standard, this can represent a clear path to reward in the form of royalties from a market that likely would not have existed without the standard being widely adopted. To balance this potential with the need for access to the patents that underlie the standard, SSOs require holders of patents on standardized technologies to license their patents on fair, reasonable, and non-discriminatory (FRAND) terms. FRAND commitments prevent the owners of patents used to implement the standard from exploiting the unearned bargaining power that they otherwise would gain as a consequence of the broad adoption of a standard. Once patented technologies incorporate into standards and a standard becomes increasingly adopted, AI developers will be compelled to use the underlying patented technology to maintain product functionality and compatibility. In exchange for making a voluntary FRAND commitment with an SSO, SEP holders gain the ability to obtain reasonable royalties from a large number of standard users that might not have existed absent the standard. Without the constraint of a FRAND commitment, SEP holders would have the same power as a monopolist that faces no competition.

Unfortunately, today an increasing number of owners of FRAND-committed SEPs are flagrantly abusing their unique position by reneging on those promises with unfair, unreasonable, or discriminatory licensing practices. These practices, under close examination by antitrust and other regulators in many jurisdictions including the United States, not only threaten healthy competition and to unbalance the standards system but also impact the viability of new markets such as AI. These abuses are amplified for small businesses because they can neither afford years of litigation to fight for reasonable royalties nor risk facing an injunction if they refuse a license that is not FRAND compliant.

NIST should, in its RMF, appropriately address how patent policies developed by SSOs today will directly impact the development of AI. SSOs vary widely in terms of their memberships, the industries and products they cover, and the procedures for establishing standards. In part due to the convergence associated with the rise of IoT, each SSO will need the ability to tailor its intellectual property policy for its particular requirements and membership. The App Association believes that some variation in patent policies among SSOs is necessary and that the U.S. government should not prescribe detailed requirements that all SSOs must

implement. At the same time, basic principles underlie the FRAND commitment and serve to ensure that standard setting is pro-competitive, and the terms of SEP licenses are in fact reasonable. Ideally, an SSO's intellectual property rights policy that requires SEP owners to make a FRAND commitment would include all of the following principles that prevent patent "hold-up" and anti-competitive conduct:

- **Fair and Reasonable to All** – A holder of a SEP subject to a FRAND commitment must license such SEP on fair, reasonable, and nondiscriminatory terms to all companies, organizations, and individuals who implement or wish to implement the standard.
- **Injunctions Available Only in Limited Circumstances** –SEP holders should not seek injunctions and other exclusionary remedies nor allowed these remedies except in limited circumstances. The implementer or licensee is always entitled to assert claims and defenses.
- **FRAND Promise Extends if Transferred** – If there is a transfer of a FRAND-encumbered SEP, the FRAND commitments follow the SEP in that and all subsequent transfers.
- **No Forced Licensing** – While some licensees may wish to negotiate a broader license agreement, patent holders should not require implementers to take licenses to patents that are not infringed, invalid, or not essential to the standard to gain access to a FRAND-encumbered SEP.
- **FRAND Royalties** – A reasonable rate for a valid, infringed, and enforceable FRAND-encumbered SEP should be based on several factors, including the value of the actual patented invention apart from its inclusion in the standard, and cannot be assessed in a vacuum that ignores the portion in which the SEP is substantially practiced or royalty rates from other SEPs required to implement the standard.

We also note that a number of SSO intellectual property rights policies require SSO participants to disclose patents or patent applications that are or may be essential to a standard under development. Reasonable disclosure policies can help SSO participants evaluate whether technologies considered for standardization are covered by patents.

The U.S. Department of Justice (DOJ) already encouraged SSOs to define FRAND more clearly. For example, DOJ's former assistant attorney general Christine Varney explained that "clearer rules will allow for more informed participation and will enable participants to make more knowledgeable decisions regarding implementation of the standard. Clarity alone does not eliminate the

possibility of hold-up…but it is a step in the right direction."[9] As another example, Renata Hesse, a previous head of the DOJ's Antitrust Division, provided important suggestions for SSOs to guard against SEP abuses.[10] NIST's planned RMF should reflect the above with respect to standards and key standards use issues including SEP licensing.

- The App Association appreciates NIST's commitment in the initial draft to have the AI RMF support organizations' abilities to operate under applicable domestic and international legal or regulatory regimes. We urge NIST to include a priority for aligning, where appropriate, with international efforts, and upon completion, promoting the NIST AI RFM for use internationally. Already, developers of AI face top-down and one-size-fits-all mandates that substantially impede their ability to develop and utilize AI across a range of use cases. It is crucial that the NIST AI RMF be offered as an alternative to such mandates, or at least have a positive influence on mandates, from other jurisdictions.

[9] Christine A. Varney, Assistant Att'y Gen., Antitrust Div., U.S. Dep't of Justice, Promoting Innovation Through Patent and Antitrust Law and Policy, Remarks as Prepared for the Joint Workshop of the U.S. Patent and Trademark Office, the Federal Trade Comm'n, and the Dep't of Justice on the Intersection of Patent Policy and Competition Policy: Implications for Promoting Innovation 8 (May 26, 2010), *available at* http://www.atrnet.gov/subdocs/2010/260101.htm.

[10] Renata Hess, Deputy Assistant Attorney General, *Six 'Small' Proposals for SSOs Before Lunch*, Prepared for the ITU-T Patent Roundtable (October 10, 2012), *available at* https://www.justice.gov/atr/speech/six-smallproposals-ssos-lunch.

The App Association appreciates NIST's consideration of the above views. AI offers immense potential for widespread societal benefit, which is why NIST's voluntary RMF should foster investment and innovation in any way practicable. Our members both use and develop solutions that include AI, and in turn, those solutions are used by countless Americans. As society moves to adopt these technologies on a greater scale, it is important that the small business developers who power a $1.3 trillion app economy can contribute to this important trend.

We urge NIST to contact the undersigned with any questions or ways that we can assist moving forward.

Sincerely,

Brian Scarpelli
Senior Global Policy Counsel

Leanna Wade
Policy Associate

ACT | The App Association
1401 K St NW (Ste 501)
Washington, DC 20005
202-331-2130

ACT | The App Association's Policy Principles for Artificial Intelligence

Artificial intelligence (AI) is an evolving constellation of technologies that enable computers to simulate elements of human thinking, such as learning and reasoning. An encompassing term, AI entails a range of approaches and technologies, such as machine learning (ML), where algorithms use data, learn from it, and apply their newly-learned lessons to make informed decisions, and deep learning, where an algorithm based on the way neurons and synapses in the brain change as they are exposed to new inputs allows for independent or assisted decision-making. Already, AI-driven algorithmic decision tools and predictive analytics have substantial direct and indirect effects in consumer and enterprise context, and show no signs of slowing in the future.

Across use cases and sectors, AI has incredible potential to improve consumers' lives through faster and better-informed decision-making, enabled by cutting-edge distributed cloud computing. Even now, consumers are encountering AI in their lives incrementally through the improvements they have seen in computer-based services they use, typically in the form of streamlined processes, image analysis, and voice recognition, all forms of what we consider "narrow" AI. These narrow applications of AI already provide great societal benefit. As AI systems, powered by streams of data and advanced algorithms, continue to improve services and generate new business models, the fundamental transformation of economies across the globe will only accelerate.

Nonetheless, AI also has the potential to raise a variety of unique considerations for policymakers. ACT | The App Association appreciates the efforts to develop a policy approach to AI that will bring its benefits to all, balanced with necessary safeguards to protect consumers.

To guide policymakers, we recommend the following principles for action:

1. **AI Strategies:** Many of the policy issues raised below involve significant work and changes that will impact a range of stakeholders. The cultural, workforce training and education, data access, and technology-related changes associated with AI will require strong guidance and coordination. National AI strategies incorporating guidance on the issues below will be vital to achieving the promise that AI offers to consumers and entire economies. We believe it is critical that countries also take this opportunity to encourage civil society organizations and private sector stakeholders to begin similar work.

2. **Research:** Policy frameworks should support and facilitate research and development of AI by prioritizing and providing sufficient funding while also ensuring adequate incentives (e.g., streamlined availability of data to developers, tax credits) are in place to encourage private and non-profit sector research. Transparency research should be a priority and involve collaboration among all affected stakeholders who must responsibly address the ethical, social, economic, and legal implications that may result from AI applications.

3. **Quality Assurance and Oversight:** Policy frameworks should utilize risk-based approaches to ensure that the use of AI aligns with the recognized standards of safety, efficacy, and equity. Providers, technology developers and vendors, and other stakeholders all benefit from understanding the distribution of risk and liability in building, testing, and using AI tools. Policy frameworks addressing liability should ensure the appropriate distribution and mitigation of risk and liability. Specifically, those in the value chain with the ability to minimize risks based on their knowledge and ability to mitigate should have appropriate incentives to do so. Some recommended guidelines include:
    - Ensuring AI is safe, efficacious, and equitable.
    - Supporting that algorithms, datasets, and decisions are auditable.
    - Encouraging AI developers to consistently utilize rigorous procedures and enabling them to document their methods and results.
    - Requiring those developing, offering, or testing AI systems to provide truthful and easy to understand representations regarding intended use and risks that would be reasonably understood by those intended, as well as expected, to use the AI solution.
    - Ensuring that adverse events are timely reported to relevant oversight bodies for appropriate investigation and action.

4. **Thoughtful Design:** Policy frameworks should require design of AI systems that are informed by real-world workflows, human-centered design and usability principles, and end-user needs. AI systems solutions should facilitate a transition to changes in the delivery of goods and services that benefit consumers and businesses. The design, development, and success of AI should leverage collaboration and dialogue among users, AI technology developers, and other stakeholders in order to have all perspectives reflected in AI solutions.

5. **Access and Affordability:** Policy frameworks should ensure AI systems are accessible and affordable. Significant resources may be required to scale systems. Policymakers should take steps to remedy the uneven distribution of resources and access and put policies in place that incent investment in building infrastructure, preparing personnel and training, as well as developing, validating, and maintaining AI systems with an eye toward ensuring value.

6. **Ethics:** The success of AI depends on ethical use. A policy framework will need to promote many of the existing and emerging ethical norms for broader adherence by AI technologists, innovators, computer scientists, and those who use such systems. Policy frameworks should:
    - Ensure that AI solutions align with all relevant ethical obligations, from design to development to use.
    - Encourage the development of new ethical guidelines to address emerging issues with the use of AI, as needed.
    - Maintain consistency with international conventions on human rights.
    - Ensure that AI is inclusive such that AI solutions beneficial to consumers are developed across socioeconomic, age, gender, geographic origin, and other groupings.
    - Reflect that AI tools may reveal extremely sensitive and private information about a user and ensure that laws protect such information from being used to discriminate against certain consumers.

7. **Modernized Privacy and Security Frameworks:** While the types of data items analyzed by AI and other technologies are not new, this analysis will provide greater potential utility of those data items to other individuals, entities, and machines. Thus, there are many new uses for, and ways to analyze, the collected data. This raises privacy issues and questions surrounding consent to use data in a particular way (e.g., research, commercial product/service development). It also offers the potential for more powerful and granular access controls for consumers. Accordingly, any policy framework should address the topics of privacy, consent, and modern technological capabilities as a part of the policy development process. Policy frameworks must be scalable and assure that an individual's data is properly protected, while also allowing the flow of information and responsible evolution of AI. This information is necessary to provide and promote high-quality AI applications. Finally, with proper protections in place, policy frameworks should also promote data access, including open access to appropriate machine-readable public data, development of a culture of securely sharing data with external partners, and explicit communication of allowable use with periodic review of informed consent.

8. **Collaboration and Interoperability:** Policy frameworks should enable eased data access and use through creating a culture of cooperation, trust, and openness among policymakers, AI technology developers and users, and the public.

9. **Bias:** The bias inherent in all data, as well as errors, will remain one of the more pressing issues with AI systems that utilize machine learning techniques in particular. Any regulatory action should address data provenance and bias issues present in the development and uses of AI solutions. Policy frameworks should:
    - Require the identification, disclosure, and mitigation of bias while encouraging access to databases and promoting inclusion and diversity.
    - Ensure that data bias does not cause harm to users or consumers.

10. **Education:** Policy frameworks should support education for the advancement of AI, promote examples that demonstrate the success of AI, and encourage stakeholder engagements to keep frameworks responsive to emerging opportunities and challenges.
    - Consumers should be educated as to the use of AI in the service they are using.
    - Academic education should include curriculum that will advance the understanding of and ability to use AI solutions.

The App Association represents more than 5,000 small business software application development companies and technology firms across the mobile economy. Our members develop innovative applications and products that meet the demands of the rapid adoption of mobile technology and that improve workplace productivity, accelerate academic achievement, monitor health, and support the global digital economy. Our members play a critical role in developing new products across consumer and enterprise use cases, enabling the rise of the internet of things (IoT). Today, the App Association represents an ecosystem valued at approximately $1.7 trillion that is responsible for millions of jobs around the world.

For more information, please visit www.actonline.org.