ACT The App Association

5 August 2024

Department for Science, Innovation and Technology
100 Parliament Street
London
SW1A 2BQ

RE: Comments of ACT | The App Association to the Department for Science, Innovation and Technology, *Open call for evidence; Cyber security of AI: call for views*

ACT | The App Association (App Association) appreciates the opportunity to submit views to the Department for Science, Innovation and Technology (DSIT) in response to its call for views on the cyber security of artificial intelligence (AI).[1] We generally support DSIT's efforts to address the cyber security of AI, including its development of a voluntary Code of Practice (which we are separately commenting on), and share the goal of helping designers, developers, users, and evaluators of AI systems evolve in knowledge, awareness, and best practices to better manage risks across the AI lifecycle.

The App Association is a trade association representing small business technology companies from across the United Kingdom (UK), European Union, and the United States. Our members are entrepreneurs, innovators, and independent developers within the global app ecosystem that engage with verticals across every industry. We work with and for our members to promote a policy environment that rewards and inspires innovation while providing resources that help them raise capital, create jobs, and continue to build incredible technology. App Association members create innovative software and hardware technology solutions and are at the forefront of incorporating AI into their products and processes.

[1] https://www.gov.uk/government/calls-for-evidence/call-for-views-on-the-cyber-security-of-ai.

AI tools are having, and will continue to have, substantial direct and indirect effects on consumers and workers. Some forms of AI are already in use to improve consumers' lives today. Moving forward, across use cases and sectors, generative AI has incredible potential to improve consumers' lives through faster and better-informed AI content creation using both distributed cloud computing and on-device processing. 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. As a further example, AI-driven software products and services revolutionised the ability of countless with disabilities to achieve experiences in their lives far closer to the experiences of those without disabilities.

While AI is already demonstrating its impressive potential, the same tools are also raising a variety of unique considerations for policymakers, including in the context of cyber security. Noting our shared goals with DSIT, we urge for alignment with the following principles and themes:

1. Harmonising and Coordinating Approaches to AI

A wide range of laws prohibit harmful conduct regardless of whether the use of AI is involved, and the use of AI does not shield companies from these prohibitions. The UK should first understand how existing frameworks apply to activities involving AI to avoid creating sweeping new authorities or agencies that awkwardly or inconsistently overlap with current policy frameworks; then, leveraging sector-specific approaches as appropriate, a coordinated and harmonised approach should be taken.

2. Quality Assurance and Oversight

Policy frameworks should utilise risk-based approaches to ensure that the use of AI aligns with any relevant recognised standards of safety, efficacy, and equity. Small software and device companies 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 minimise risks based on their knowledge and ability to mitigate should have appropriate incentives to do so. Some recommended areas of focus include:

- Ensuring AI is safe, efficacious, and equitable.
- Encouraging AI developers to consistently utilise rigorous procedures and enabling them to document their methods and results.

- Encouraging those developing, offering, or testing AI systems intended for consumer use 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.

3. Thoughtful Design

Policy frameworks should encourage design of AI systems that are informed by real-world workflows, human-centered design and usability principles, and end-user needs. AI systems 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 to have all perspectives reflected in AI solutions.

4. Access and Affordability

Policy frameworks should enable products and services that involve AI systems to be accessible and affordable. Significant resources may be required to scale systems. Policymakers should also ensure that developers can build accessibility features into their AI-driven offerings and avoid policies that limit their accessibility options.

5. Bias

The bias inherent in all data, as well as errors, will remain one of the more pressing issues with AI systems that utilise machine learning techniques in particular. Regulatory agencies should examine data provenance and bias issues present in the development and uses of AI solutions to ensure that bias in datasets does not result in harm to users or consumers of products or services involving AI, including through unlawful discrimination.

6. Research and Transparency

Policy frameworks should support and facilitate research and development of AI by prioritising and providing sufficient funding while also maximising innovators' and researchers' ability to collect and process data from a wide range of sources. Research on the costs and benefits of transparency in AI should also be a priority and involve collaboration among all affected stakeholders to develop a better understanding of how and under which circumstances transparency mandates would help address risks arising from the use of AI systems.

7. Modernised Privacy and Security Frameworks

The many new AI-driven uses for data, including sensitive personal information, raise privacy questions. They also offer the potential for more powerful and granular privacy 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. A balanced framework should avoid undue barriers to data processing and collection while imposing reasonable data minimisation, consent, and consumer rights frameworks.

8. Ethics

The success of AI depends on ethical use. A policy framework must promote many of the existing and emerging ethical norms for broader adherence by AI technologists, innovators, computer scientists, and those who use such systems. Relevant ethical considerations include:

- Applying ethics to each phase of an AI system's life, from design to development to use.
- Maintaining consistency with international conventions on human rights.
- Prioritising inclusivity such that AI solutions benefit consumers and are developed using data from 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 require the protection of such information.

9. 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(s) they are using.
- Academic education should include curriculum that will advance the understanding of and ability to use AI solutions.

10. Intellectual Property

The protection of intellectual property (IP) rights is critical to the evolution of AI. In developing approaches and frameworks for AI governance, policymakers should ensure that compliance measures and requirements do not undercut safeguards for IP or trade secrets.

The App Association also urges DSIT to align with our recommendations contained in our AI Roles and Interdependencies Framework. This document proposes clear definitions of stakeholders across the healthcare AI value chain, from development to distribution, deployment, and end use; and discusses roles for supporting safety, ethical use, and fairness for each of these important stakeholder groups that are intended to illuminate the interdependencies between these actors, thus advancing the shared responsibility concept. This framework is appended to this comment letter.

The App Association appreciates DSIT's consideration of the above views. We urge DSIT to contact the undersigned with any questions or ways that we can assist moving forward.

Sincerely,

Brian Scarpelli
Senior Global Policy Counsel

Stephen Tulip
UK Country Manager

Chapin Gregor
Policy Counsel

ACT | The App Association

ACT | The App Association AI Roles & Interdependency Framework

Overview: Artificial Intelligence (AI), especially generative AI, is already a powerful tool for consumers and companies. App Association small business members have a vital role in advancing AI's positive impacts by identifying new and novel opportunities where the responsible use of AI can solve expensive problems and provide new efficiencies for consumers and businesses.

While AI capabilities are already positively transforming American society, the App Association also recognizes that the same capabilities raise unique challenges that the government, private sector, and others have an important role in addressing across development, distribution, deployment, and end use phases. The App Association has worked proactively with its diverse and innovative community of small businesses to develop this consensus taxonomy, which describes the roles and interdependencies of various actors in the value (or supply) chain of AI solutions. These roles include several AI/ML developer subgroups, deploying organizations, end users, standard-setting organizations, certification and test beds, specialty boards and licensing bodies, and academic institutions. Many of these stakeholders map to actors in the National Institute for Standards and Technology's (NIST's) AI Risk Management Framework (RMF), which we indicate on the far right of the matrix below.

While the App Association has created comprehensive policy principles for AI governance, there we have several recommendations from this roles and interdependencies document. **The App Association recommends: (1) that requirements placed on small business AI developers and users be based on demonstrated harms; (2) the leveraging of a risk-based approach to AI harm mitigation where the level of review, assurance, and oversight is proportionate to those demonstrated harms; and (3) that those in AI value chains with the ability to minimize risks based on their knowledge and ability have appropriate responsibilities and incentives to do so.**

ACT | The App Association AI Roles & Interdependency Framework

Stakeholder Group	Definition	Roles	NIST AI RMF Actor Tasks
AI/ML Developers	Someone who designs, codes, researches, or produces an AI/ML system or platform for internal use or for use by a third party. **See below for defined Subgroups of this Stakeholder Group along with recommendations specific to that Subgroup.**	• Informing deployers and users of data requirements/definitions, intended use cases/populations and applications (e.g., disclosing sufficient detail allowing providers to determine when an AI-enabled tool should reasonably apply to the individual they are treating), including whether the AI/ML tools are intended to augment human work versus automate workflows, and status of/compliance with all applicable legal and regulatory requirements. • Prioritizing safety, effectiveness, transparency, data privacy and security, and equity from the earliest stages of design, leveraging (and, where appropriate, updating) existing AI/ML guidelines on research and ethics, leading standards, and other resources. • Employing algorithms that produce repeatable results and, when feasible, are auditable, and make decisions that comply with relevant sector-specific requirements. • Using risk management approaches that scale to the potential likely harms posed in intended use scenarios to support safety, protect privacy and security, avoid harmful outcomes due to bias, . • Providing information that enables those further down the value chain can assess the quality, performance, equity, and utility of AI/ML tools. • Aligning with relevant ethical obligations and international conventions on human rights and supporting the development of new ethical guidelines to address emerging issues.	AI Deployment; Operation and Monitoring; Test, Evaluation, Verification, and Validation (TEVV); Human Factors; Domain Expert; AI Impact Assessment; Governance and Oversight

Stakeholder Subgroup	Definition	Roles	NIST RMF Actor Tasks
Foundation Model Developer	Someone who creates or modifies large and generalizable machine learning models that can be	***Building on the cross-AI/ML Developer roles noted above:*** • Assessing what bias and safety issues might be present in its Foundation Model,	AI Deployment; Operation and Monitoring; Test, Evaluation, Verification, and Validation (TEVV); Human Factors;

Stakeholder Subgroup	Definition	Roles	NIST RMF Actor Tasks
	used/adapted for various downstream tasks and applications, such as natural language processing, computer vision, or software development.	and documenting steps taken to mitigate those issues in its Transparency Documentation (e.g., Transparency Notes, System Cards and product documentation). • Providing clear guidance on (1) how to use and adapt its Foundation Model for various foreseeable downstream tasks and applications, and (2) what limitations or risks may arise from doing so based on challenges discovered during testing and deployment.	Domain Expert; AI Impact Assessment; Governance and Oversight
AI Platform Developer	Someone who leverages existing foundation models and builds an industry-agnostic platform that enables other developers to access, customize, and deploy these models for various use cases and applications, such as natural language processing, computer vision, and/or software development.	***Building on the cross-AI/ML Developer roles noted above:*** • Testing for, identifying, and mitigating bias and safety issues that may arise from using or modifying existing foundation models for its AI Platform, and documenting these issues and steps taken to address them in its transparency documentation (e.g., transparency notes, system cards and product documentation).	AI Deployment; Operation and Monitoring; Test, Evaluation, Verification, and Validation (TEVV); Human Factors; Domain Expert; AI Impact Assessment; Governance and Oversight
Use Case AI Platform Developer	Someone who creates or uses AI-powered platforms that are tailored for a particular domain or sector. These platforms may leverage foundation models (or other types of machine learning models or solutions), such as AI platforms, that are suitable for domain-specific	***Building on the cross-AI/ML Developer roles noted above:*** • Meeting specific requirements and standards of the domain to address unique accuracy, efficacy, explainability, and compliance needs. • Testing for, identifying, and mitigating any bias and safety issues that may affect domain-specific outcomes or performance needs, and documenting these issues and the steps it has taken to address them in its transparency	AI Deployment; Operation and Monitoring; Test, Evaluation, Verification, and Validation (TEVV); Human Factors; Domain Expert; AI Impact Assessment; Governance and Oversight

Stakeholder Subgroup	Definition	Roles	NIST RMF Actor Tasks
	problems and data sources.	documentation (e.g., transparency notes, system cards and product documentation).	
AI Solution Developer	Someone who creates complete digital tools and technologies for a domain. They may build or incorporate AI solutions with both use case AI platforms, which are specialized for the domain, and AI platforms, which are more general and adaptable for various use cases and applications.	***Building on the cross-AI/ML Developer responsibilities noted above:*** • Specifying appropriate uses for its solution to avoid amplifying bias or safety issues that may exist in the underlying foundation models, AI platforms, or domain-specific AI platforms. • Designing user interfaces to enable an end user to safely and effectively act upon the output of the tool, such as providing explanations, feedback mechanisms, or human oversight options, providing clear documentation to Deploying Organizations and Users to help them avoid bias and safety issues.	AI Deployment; Operation and Monitoring; Test, Evaluation, Verification, and Validation (TEVV); Human Factors; Domain Expert; AI Impact Assessment; Governance and Oversight

Stakeholder Group	Definition	Roles	NIST AI RMF Actor Tasks
Deploying Organization	Someone who is deploying solutions built by AI Solution Developers. They may also have their own internal IT staff that employ use case AI platforms or general AI platforms to develop their own custom AI solutions.	*Respecting that managing AI/ML risks will be more challenging for small to medium-sized organizations depending on their capabilities and resources:* • Adopting AI/ML Developer instructions for use, specifying appropriate uses for Users through governance policies to avoid bias and safety issues that may exist in the underlying foundation models, AI platforms, or use case AI platforms. • Developing and leveraging solutions that augment efficiencies in automation, facilitate administrative simplification/reduce workflow burdens, and are fit for purpose. • Setting organization policy/designing workflows to reduce the likelihood that a User will act upon the output	AI Deployment; Operation and Monitoring; Domain Expert; AI Impact Assessment; Procurement; Governance and Oversight

Stakeholder Group	Definition	Roles	NIST AI RMF Actor Tasks
		of the tool in a way that would cause fairness/bias or safety issues (tailored explanations, feedback mechanisms, and/or human oversight options). • Assuring that AI/ML systems allow for the individualized assessment of domain-specific circumstances and flexibility to override automated decisions, ensuring that use of AI/ML does not improperly reduce or withhold intended benefits or inappropriately override human judgement. • Developing support mechanisms for the use of AI/ML by providers based on validation, aligning with decision-making processes familiar to the domain and high-quality evidence. • Developing organizational guidance on how the AI solution should and should not be used. • Creating engagement pathways to support dialogue with AI use case developers, AI solution developers, or any other applicable AI/ML developer, to enable ongoing updates to address evolving risks and benefits of AI solution uses. • Creating risk-based, tailored communications and engagement plans to enable easily understood explanations to customers about how the AI solution was developed, its performance and maintenance, and how it aligns with the latest best practices and regulatory requirements.	
AI End Users	Someone who directly interacts with or benefits from the AI solutions that are built by AI Solution Developers or by the internal IT staff of the Deploying Organization.	*Respecting that managing AI/ML risks will be more challenging for small to medium-sized organizations depending on their capabilities and resources:* • Aligning with consensus AI/ML definitions, present-day and future AI/ML solutions, the future of AI/ML changes and trends. • Taking required training and incorporating employer guidance about use of AI/ML solutions. • Documenting (through automated processes or otherwise) and reporting any issues or feedback to the	AI Deployment; Operation and Monitoring; Domain Expert; AI Impact Assessment; Procurement; Governance and

Stakeholder Group	Definition	Roles	NIST AI RMF Actor Tasks
		developer, such as errors, vulnerabilities, biases, or harms (where AI/ML's use is known by the User). • Ensuring there is appropriate review of the output or recommendations from each AI solution prior to acting on it to make decisions, if relevant (where AI/ML's use is known by the User). • Raising awareness of and acting according to customers' rights and choices when using AI solutions, such as consent, access, correction, or deletion of their personal data.	Oversight; Human Factors
Standard-Setting Organizations	An organization whose primary function is developing, coordinating, promulgating, revising, amending, reissuing, interpreting, or otherwise contributing to the usefulness of technical standards to those who employ them.	• Developing and promoting adoption of international voluntary/non-regulatory consensus standardized approaches and resources to steward a shared responsibility approach to technology standards that include or are otherwise related to AI.	Human Factors; Domain Expert; AI Impact Assessment; Governance and Oversight
Certification Bodies & Test Beds	A certification body is a third-party organization that assures the conformity of a product, process or service to specified requirements. A test bed is a platform for conducting rigorous, transparent, and replicable testing of scientific theories, computing tools, and new technologies to a standard.	• Creating and making available transparent and reliable processes for the assurance of conformity to voluntary AI standards. • Creating and making available voluntary sandbox environments to help evaluate the usability and performance of AI/ML-based high-performance computing applications to advance the understanding of how reliable and efficacious AI, and to provide an appropriate assurance of reliability and efficacy.	Test, Evaluation, Verification, and Validation (TEVV); Human Factors; Domain Expert; AI Impact Assessment; Governance and Oversight
Accrediting and Licensing Bodies, Specialty Societies and Boards	Accrediting and licensing bodies are governing authorities that establish the suitability of any participating certification body. Notably, state-level boards serve	• Based on needs and expertise, developing and setting the standard of practice/behavior and ethical guidelines to address emerging issues with the use of AI/ML in the relevant domain. • Identifying the most appropriate uses of AI-enabled technologies and developing and disseminating	Test, Evaluation, Verification, and Validation (TEVV); Human

Stakeholder Group	Definition	Roles	NIST AI RMF Actor Tasks
	this purpose for certain professions to standards set by each state. Specialty societies are organizations for specialized professionals.	guidance and education on the responsible deployment of AI/ML, both generally and for specialty-specific uses.	Factors; Domain Expert; AI Impact Assessment; Governance and Oversight
Academic Education Institutions	Tertiary educational institutions, professional schools, or forms a part of such institutions, that teach and award professional degrees.	• Developing and teaching curriculum that will advance understanding of and ability to use AI/ML solutions responsibly, which should be assisted by inclusion of data scientists and engineers as instructors as needed. • Developing curriculum to advance the understanding of data science research to help inform ethical bodies.	Human Factors; Domain Expert; AI Impact Assessment