BEFORE THE
DEPARTMENT OF COMMERCE
National Institute of Standards and Technology
WASHINGTON, D.C. 20230

In the Matter of	)	
	)	
Request for Information (RFI) Related to	)	
NIST's Assignments Under Sections 4.1, 4.5	)	Docket No. 231218-0309
and 11 of the Executive Order Concerning	)	
Artificial Intelligence (Sections 4.1, 4.5, and 11)	)	
	)	

COMMENTS OF USTELECOM – THE BROADBAND ASSOCIATION

USTelecom – The Broadband Association ("USTelecom")[1] submits these comments in response to the National Institute of Standards and Technology ("NIST") request for information concerning its various assignments under Executive Order 14110, Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence.

We appreciate NIST's thought leadership on artificial intelligence ("AI"), including generative AI, and in these comments we make a variety of suggestions to advance effective AI risk management. Notably, we emphasize the distinct roles and responsibilities of deployers and developers. We also discuss various nascent tools to mitigate risk and we recommend that NIST adopt the most recent definition of AI developed by the Organisation for Economic Co-operation and Development ("OECD").

USTelecom's long history of collaboration with U.S. government partners informs our comments in this proceeding. USTelecom presently chairs the Communications Sector

[1] USTelecom is the nation's leading trade association representing service providers and suppliers for the telecom industry. USTelecom members provide a full array of services, including broadband, voice, data, and video over wireline and wireless networks. Its diverse member base ranges from large international publicly traded communications corporations to local and regional companies and cooperatives, serving consumers and businesses in every corner of the country and world.

Coordinating Council ("CSCC") and co-chairs the Information and Communication Technology ("ICT") Supply Chain Risk Management Task Force ("SCRM Task Force"), the two principal organizations that serve as the government's industry partners for developing cybersecurity and supply chain security policies.

USTelecom founded, and co-leads with the Consumer Technology Association, the Council to Secure the Digital Economy ("CSDE"), a group of fifteen large international ICT companies recognized by the U.S. government as a leading industry partnership in coordinating efforts to combat botnets, respond to cyber crises, and promote security through development of best practices that influence the development of standards.

I. INTRODUCTION

The recent proliferation of new AI technology represents a frontier of human innovation, analogous to the earliest days of consumer access to the internet. As policymakers work to develop a regulatory framework to address potential heightened risks posed by new uses of AI, USTelecom takes this opportunity to offer the following recommendations for your consideration.

II. TO ADVANCE EFFECTIVE AI RISK MANAGEMENT, REGULATORY OBLIGATIONS SHOULD BE TAILORED TO THE SPECIFIC ROLES OF DEPLOYERS AND DEVELOPERS

While all AI actors share responsibilities for ensuring AI is trustworthy and fit for purpose,[2] it is incumbent on policymakers to recognize the different roles developers and deployers play in the AI life cycle, and to align policy and regulatory obligations accordingly.

[2] NIST RMF at 6.

Developers research, design, code, and produce AI systems for use by deployers and end users.[3] More specifically, a "Developer" is a natural or legal person, public authority, agency or other body that provides the initial infrastructure, or substantial modification to, an AI system, including model building and interpretation tasks, that involve the creation, selection, calibration, training, and/or testing of models or algorithms. Developers of AI systems and models most often have sole knowledge of the code used to develop an AI system. Developers also have control over any and all related data used to train the AI, the training methods, and guardrails for ensuring models delivered to deployers are safe, secure, legal, effective, and trustworthy, and that they minimize the potential for bias and discrimination. While developers generally do not have control over subsequent uses of an AI system by a deployer, the developer is the only entity that can shed light on the intended uses of AI systems for deployers and policymakers, and that can take the steps in model development, data selection, and guardrail implementation that are appropriate for those intended uses.

In contrast, deployers use an AI system produced by a developer. Deployers may modify or adjust AI systems to maximize or tailor the system to their business purposes, but "do[ ] not generally have control over design decisions made by another company that developed the AI system."[4] Deployers may use AI systems internally, or they may use them to engage with consumers or end users. In those instances where deployers are using AI systems directly with consumers, they will need to rely substantially on the information provided by, and decisions

[3] See AI Developers and Deployers: An Important Distinction, BSA - The Software Alliance (Mar. 16, 2023); see also NIST RMF 1.0 at 35 ("AI Development actors provide the initial infrastructure of AI systems and are responsible for model building and interpretation tasks, which involve the creation, selection, calibration, training, and/or testing of models or algorithms.").

[4] AI Developers and Deployers: An Important Distinction, BSA - The Software Alliance (Mar. 16, 2023).

made by, the developers. Absent regulatory or contractual transparency obligations for developers, deployers will have little understanding of what comprises an AI system or the universe of expected outcomes from the use of a particular AI system.

The distinction between developers and deployers has been recognized at the international level, including the G7 and EU. While the G7 International Guiding Principles on Artificial Intelligence apply across the ecosystem, the G7 Code of Conduct is aimed exclusively at developers recognizing the unique responsibility that organizations developing Advanced AI systems have to promote safe, secure, and trustworthy AI worldwide. Likewise, the EU AI Act applies horizontally to providers, manufacturers, importers, distributors, and deployers of AI systems in all sectors and industries, but significant obligations are placed on developers (providers) in recognition of the information asymmetry that exists between developers and deployers–(even for developers not established in the EU).[5]

As a result, policymakers must recognize the different roles and responsibilities of developers and deployers of AI systems and align regulatory obligations with the information available to each stakeholder and at relevant points in the AI life cycle. This approach is critical to ensuring regulatory obligations are tailored to an organization's role in the AI marketplace, and that both are held to responsible AI practices.

[5] The EU AI Act places distinct and separate responsibilities on providers (those who develop AI) and deployers. For high risk systems, providers must undergo the relevant conformity assessment procedure, prior to placing high-risk AI systems on the market as well as other various obligations. The main responsibility for deployers of high-risk AI is to ensure they use such systems in accordance with the instructions of use. There are additional specific obligations for deployers in certain high risk use cases. Likewise, developers and deployers have scaling degrees of responsibilities with respect to transparency requirements for AI systems that interact directly with humans and certain GPAI models. In the low risk category which encompasses general purpose AI models, developers are still subject to a number of requirements, while deployers are exempt.

Upfront Obligations, Backend Liability, and Responsible Party. Three key policy questions to address in the context of this issue are: (1) What are the appropriate upfront obligations for developers and deployers? (2) What is the appropriate structure for liability on the backend? (3) When does a deployer become a developer, when is a developer also a deployer, and who is the responsible party when the lines are blurred? The regulatory construct for upfront obligations, backend liability, and how these roles are defined should be approached thoughtfully and with continued industry input.

Upfront Obligations. With regard to the appropriate upfront obligations for developers and deployers, particularly in higher-risk applications of AI, policymakers should recognize that developers have the most insight into how an AI is trained, what the AI can and cannot do, and what safeguards were put in place to mitigate bias, discrimination, and other negative outcomes.

Developers. Given the significant–and asymmetrical–access to information developers have about the inner functioning of AI systems, upfront obligations for developers should include extensive transparency requirements to deployers in the form of a detailed model/system card and any additional contextual information around what uses are considered on-label and off-label. Developers of AI systems should be held responsible for ensuring the systems meet those specifications. Model/System cards provided to deployers should include at a minimum:

- **Model Details:** A brief narrative explaining what the model does, any outputs, proof of concept, date, version, model type, and underlying licenses.
- **Use Cases:** What uses are intended and not intended, and any mitigation controls put in place to prevent unintended outcomes for intended uses.

- **Limitations & Risks:** Developers should flag any known limitations. They should also highlight any known, likely, and specific high risks for using an AI system and appropriate steps for risk mitigation.
- **Training:** Data sources, data strategy, and permission to use.
- **Analyses:** Evaluation metrics, fairness, and known recommendations.

Deployers. With regard to deployers, upfront obligations may include a requirement to notify the developer in instances where the deployer wants to use the AI system in a way that was not contemplated in the original commercial agreement. Deployers should also be responsible for post-deployment monitoring and relevant safeguards put in place for AI systems deployed for the purpose of direct consumer engagement.

Responsible Party. In some cases, an entity will act both as a developer and deployer. Under those circumstances, the entity should observe the responsibilities of both, executing its role-specific obligations based on the context.

There may be times when a deployer modifies an AI system substantially and in a way that is prohibited by, or outside the boundaries of, the model/system card provided by the developer to the deployer. Under those circumstances, the deployer assumes the obligations of a developer with respect to its modifications. The standard for when a deployer assumes the obligations of a developer through substantial modification to an AI system should be fairly high. For example, deployers should not incur developer obligations by training or using an AI on their own data or making predictable and/or necessary modifications to AI systems as required to carry out or optimize the expected functioning of the AI. (Predictable modifications include re-training and scoring, for example.)

A developer acts as a deployer any time it uses AI systems that it developed itself for its own internal business operations or to engage with consumers or end users directly.

Backend Liability. There will likely be some level of shared liability depending on a number of contributing factors, e.g., the level of harm resulting from an AI malfunction, whether the AI use was an intended use, if the resulting harm was predictable/ascertainable by the developer and whether adequate measures were put in place before the AI system was provided to deployers. These theories of liability stem from historical product liability or tort principles. Based on the discussion above, however, there is a need for certain protections to be put in place. A deployer should be protected from liability if it makes AI systems available to end users as intended and as described in the documentation provided by the developer and the AI malfunctions in a way that could have been prevented by the developer, or when a deployer relies on a model/system card provided by a developer to the deployer's detriment.

III. AI RED TEAMING IS NOT A SILVER BULLET, BUT CAN BE HELPFUL AS PART OF A COMPREHENSIVE GOVERNANCE FRAMEWORK

AI red teaming is still a nascent concept/practice. While it is helpful, it is not a silver bullet that should replace other assurance measures.

AI Red Teaming Undefined. There is currently no generally accepted definition for AI red teaming, as the concept has a number of variables, including (1) which party performs the AI red teaming; (2) what scope they are testing with the AI red teaming exercise—i.e., safety, security, utility, efficiency, abuse, etc.; (3) what AI red teaming best practices and requirements look like; and (4) the intended outcome of AI red teaming—e.g., to determine if retraining/fine-tuning or UI redesign is required, or something else.

Not a Silver Bullet. AI red teaming is not a silver bullet and it cannot solve all generative AI risk; AI red teaming is about assurance rather than accountability. Red teaming can only test if an AI system provides the intended outcome under normal circumstances or stress testing. As a result, policymakers will still need to ensure accountability best practices are part of a comprehensive governance framework.

IV. AI CONTENT AUTHENTICATION AND PROVENANCE TECHNIQUES ARE EVOLVING, BUT PRESENTLY HAVE VARIOUS LIMITATIONS

AI content authentication and provenance tools, while increasingly sophisticated, have several limitations that prevent them from being a panacea. Notably, if the source data or provenance information of content can be manipulated or spoofed, it undermines the reliability of authentication tools that rely on this data.

As AI and machine learning technologies evolve, so, too, do the methods for creating deepfakes and other manipulated content. This constant evolution can create a cat-and-mouse scenario where authentication tools are always trying to catch up with the latest techniques used by forgers.

AI tools can make errors, resulting in false positives (identifying authentic content as fake) or false negatives (failing to identify fake content). Understanding the context in which content was created and distributed is crucial for authentication. This often requires human expertise and cannot be entirely replaced by AI, especially in complex or ambiguous cases.

V. TO PROMOTE INTERNATIONAL HARMONIZATION AND COOPERATION, THE U.S. GOVERNMENT SHOULD ADOPT THE OECD'S MOST RECENT DEFINITION OF AI

For governments to effectively create laws and regulations pertaining to AI, and for consumers to trust AI systems, policymakers should adopt a foundational definition for AI.

Considering the international scope of AI, consensus on a uniform definition among governments around the world would facilitate better cooperation and compatibility across regions.

USTelecom advises the U.S. government to adopt the definition of AI advanced and recently updated by the OECD, which has 38 member countries: "*An AI system is a machine-based system that for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments. Different AI systems vary in their levels of autonomy and adaptiveness after deployment*."[6]

In general, we encourage the U.S. government to remain engaged with global stakeholders and minimize definitional barriers to interoperability or economies of scale absent compelling reasons.

VI. CONCLUSION

USTelecom welcomes the continuation of this critical dialogue and thanks NIST for the opportunity to share our insights. We look forward to working with our U.S. government partners to promote and implement safe, ethical, and trustworthy AI systems.

[6] OECD AI Policy Observatory, *Updates to the OECD's Definition of an AI System Explained* (Nov. 29, 2023), https://oecd.ai/en/wonk/ai-system-definition-update.

Respectfully submitted,

/s/ Paul Eisler

Paul Eisler
Vice President, Cybersecurity

USTelecom – The Broadband Association
601 New Jersey Avenue, NW
Suite 600
Washington, DC 20001
(202) 326-7300

February 2, 2024