Center for AI and Digital Policy

Comments of

THE CENTER FOR AI AND DIGITIAL POLICY (CAIDP)

To

NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION (NTIA)

Regarding

ARTIFICIAL INTELLIGENCE (AI) SYSTEMS
ACCOUNTABILITY MEASURES AND POLICIES

We write to you, on behalf of the Center for AI and Digital Policy (CAIDP), in response to the Request for Comments (RFC) issued by the NTIA on Artificial Intelligence ("AI") system accountability measures and policies.[1] In the Comments below we (1) provide General Recommendations on AI Accountability and (2) provide specific responses to Questions 1, 4, 5, 9, 16, 20, 25, 26, and 34.

In summary, we recommend:

1. **Companies should not release AI products that are not safe.** President Biden has said directly, at least twice, that tech companies have a responsibility to make sure their products are safe before making them public.[2]

2. **Human-centric accountability practices must protect fundamental rights, democratic values, and the rule of law.**

---

[1] Notice, Request for Comment, *Artificial Intelligence (AI) Systems Accountability Measures and Policies,* National Telecommunications and Information Administration, U.S. Department of Commerce, 88 FR 22433, https://www.federalregister.gov/documents/2023/04/13/2023-07776/ai-accountability-policy-request-for-comment. See also, CAIDP, Public Voice, *NTIA, Request for Comments– AI Accountability*, https://www.caidp.org/public-voice/ntia-ai-accountability-us-2023-1/

[2] The White House, *Remarks by President Biden in Meeting with the President's Council of Advisors on Science and Technology,* (April 4, 2023), https://www.whitehouse.gov/briefing-room/speeches-remarks/2023/04/04/remarks-by-president-biden-in-meeting-with-the-presidents-council-of-advisors-on-science-and-technology/; The White House, *Readout of White House Meeting with CEOs on Advancing Responsible Artificial Intelligence Innovation*, (May 4, 2023) ("President Biden dropped by the meeting to underscore that companies have a fundamental responsibility to make sure their products are safe and secure before they are deployed or made public.), https://www.whitehouse.gov/briefing-room/statements-releases/2023/05/04/readout-of-white-house-meeting-with-ceos-on-advancing-responsible-artificial-intelligence-innovation/

3. **Accountability mechanisms must incorporate best practices** set out in the Universal Guidelines for Artificial Intelligence[3], the OECD AI Principles[4] and the UNESCO Recommendation on AI Ethics[5].

4. **Accountability should be based on mandatory impact assessments,** audits, and certifications throughout the AI lifecycle to ensure transparency, auditability, contestability, and traceability.

5. **Legal standards should be established to ensure AI accountability.** Accountability mechanisms or practices will have no meaningful impact in the absence of clearly defined legal standards and enforceable remedies.

6. **The United States should support a comprehensive international treaty for AI to ensure accountability across the public and private sectors**.[6]

The CAIDP is an independent research and education non-profit, incorporated in Washington, DC. We are a global network of AI policy experts and advocates. We advise national governments and international organizations regarding artificial intelligence and digital policy.[7] We set out below our general recommendations on AI system accountability and specific comments to the questions presented in your RFC.

CAIDP General Recommendations on AI Accountability

At the outset we would like to highlight that the United States has expressed formal commitment to the OECD AI Principles that clearly set out accountability objectives. Our General Recommendations for accountability of AI Systems is as follows:

1*. Enactment of federal legislation for accountability of AI systems incorporating the Universal Guidelines for AI, the OECD AI Principles, and the UNESCO Recommendation for AI Ethics.*

The Organization for Economic Cooperation and Development (OECD) in 2019 promulgated the OECD Principles on Artificial Intelligence which was adopted by both member and non-member countries. The United States has endorsed the OECD AI Principles[8]. According to the OECD AI Principle on Accountability (1.5): "*AI actors should be*

---

[3] Universal Guidelines for Artificial Intelligence**,** https://thepublicvoice.org/ai-universal-guidelines/
[4] Recommendation of the Council on Artificial Intelligence, OECD (May 21, 2019), https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449
[5] UNESCO Recommendation on the Ethics of AI 2021, https://unesdoc.unesco.org/ark:/48223/pf0000377897
[6] CAIDP, Council of Europe AI Treaty, https://www.caidp.org/resources/coe-ai-treaty/
[7] CAIDP, https://www.caidp.org
[8] *U.S. Joins with OECD in Adopting Global AI Principles,* NTIA (May 22, 2019), https://www.ntia.doc.gov/blog/2019/us-joins-oecd-adopting-global-ai-principles

accountable for the <u>proper functioning</u> of AI systems and for the respect of the above principles, based on their roles, the context, and consistent with the state of art." (emphasis added)

The Universal Guidelines for Artificial Intelligence ("UGAI") is a framework for AI governance based on the protection of human rights and was adopted in 2018 by the International Conference on Data Protection and Privacy Commissioners. The UGAI has been endorsed by more than 300 experts and 70 organizations in 40 countries. According to the UGAI Assessment and Accountability Obligation, "*An AI system should be deployed only after an adequate evaluation of its purpose and objectives, its benefits, as well as its risks. Institutions must be responsible for decisions made by an AI system.*"[9]

2. *Implementation of the accountability provisions of the AI Bill of Rights*[10]

(a) The principle requires accountability from automated decision-making systems and states that, "the individual or organization responsible for the system" be clearly identified and explanation be afforded as to "how and why an outcome impacting you was determined by an automated system."

(b) President Biden has already set out an important and necessary agenda for the governance of AI. He has called for new legislation to govern AI that would provide greater transparency and reduce the risk of algorithmic discrimination.[11] The President wrote that it was time to hold Big Tech companies accountable for the algorithms they use and called for bipartisan legislation to protect privacy, promote competition, and safeguard children.[12] The President also issued Executive Order 13985 to promote racial equity and support underserved communities through the federal government.[13] He specifically urged federal agencies to "prevent and remedy discrimination, including by protecting the public from algorithmic discrimination."

---

[9] UGAI Guideline 5

[10] The White House, *Blueprint for An AI Bill of Rights*, https://www.whitehouse.gov/ostp/ai-bill-of-rights/

[11] Joe Biden, *Republicans and Democrats, Unite Against Big Tech Abuses,* Wall Street Journal, (January 11, 2023), https://www.wsj.com/articles/unite-against-big-tech-abuses-social- media-privacy-competition-antitrust-children-algorithm-11673439411

[12] CAIDP Update 5.02, January 16, 2023, https://www.caidp.org/app/download/8435896763/CAIDP-Update_5.02.pdf

[13] The White House, *Executive Order on Further Advancing Racial Equity and Support for Underserved Communities Through The Federal Government*, February. 16, 2023 https://www.whitehouse.gov/briefing-room/presidential-actions/2023/02/16/executive- order-on-further-advancing-racial-equity-and-support-for-underserved-communities- through-the-federal-government/

CAIDP Specific Responses to Questions in RFC

A. AI Accountability Objectives (Responses to Questions 1, 4,5)

1. What is the purpose of AI accountability mechanisms such as certifications, audits, and assessments?

The Explanatory Memorandum[14] to the UGAI states as follows:

"The Assessment and Accountability Obligation speaks to the obligation <u>to assess an AI system prior to and during deployment.</u> Regarding assessment, it should be understood that a central purpose of this obligation is to determine whether an AI system should be established. If an assessment reveals substantial risks, such as those suggested by principles concerning Public Safety and Cybersecurity, then the project should not move forward."

We recommend that the overriding objective of AI accountability mechanisms such as certifications, audits, and assessments should be to determine whether an AI system should be deployed. Credible assurance of AI systems could be through certification programs under Federal AI legislation based on the established governance frameworks outlined above. Even the NIST AI Risk Management Framework is voluntary which does not set adequate and appropriate incentives for accountability.

4. Can AI accountability mechanisms effectively deal with systemic and/or collective risks of harm, for example, with respect to worker and workplace health and safety, the health and safety of marginalized communities, the democratic process, human autonomy, or emergent risks?

AI accountability mechanisms must take into account human rights, privacy protections, safety (including public safety), security (including cybersecurity), data quality, accuracy, transparency and reliability obligations to address system or collective risks of harm. The Joint Statement issued by federal agencies[15] also point to these criteria for enforcement of accountability of AI systems. We also recommend consulting the *Artificial Intelligence and Democratic Values Index* (AIDV).[16] The AIDV report specifically calls out red lines for

---

[14] *Universal Guidelines for Artificial Intelligence*, Explanatory Memorandum and References, (October 2018), https://thepublicvoice.org/ai-universal-guidelines/memo/

[15] *Joint Statement on Enforcement Efforts Against Discrimination and Bias in Automated Systems*, https://www.eeoc.gov/joint-statement-enforcement-efforts-against-discrimination-and-bias-automated-systems

[16] Center for AI and Digital Policy, *Artificial Intelligence and Democratic Values Index* (2022), https://www.caidp.org/reports/aidv-2022/

certain AI technologies such as facial recognition and other biometric technologies that present potential for privacy violations, abusive practices like mass surveillance, discriminatory classifications, and social scoring.

The UNESCO Recommendation on Ethics of AI[17] state the following criteria that must be considered by accountability mechanisms to protect collective or societal interests:

- AI systems **should not segregate, objectify, or undermine freedom and autonomous decision-making as well as the safety of human beings and communities**, divide and turn individuals and groups against each other, or threaten the coexistence between humans, other living beings and the natural environment. (Rec #24)

- AI system use must not violate or abuse human rights; and the AI method should be **appropriate to the context and should be based on rigorous scientific foundations.** In scenarios where decisions are understood to have an impact that is irreversible or difficult to reverse or may involve life and death decisions, **final human determination** should apply. In particular, AI systems should not be used for social scoring or mass surveillance purposes (Rec #26)

- All actors involved in the life cycle of AI systems must **comply** with applicable international law and domestic legislation, standards and practices. They should reduce the **environmental impact of AI systems**. (Rec #18)

- Appropriate **oversight, impact assessment, audit and due diligence mechanisms, including whistle-blowers' protection**, should be developed to ensure accountability for AI systems and their impact throughout their lifecycle. (Rec #43)

- Governments should adopt a regulatory framework that sets out a procedure, particularly for public authorities, to carry out **ethical impact assessments on AI systems to predict consequences, mitigate risks, avoid harmful consequences, facilitate citizen participation and address societal challenges**. The assessment should also establish appropriate oversight mechanisms, including auditability, traceability and explainability, which enable the assessment of algorithms, data and design processes, as well as include external review of AI systems. (Rec #53)

5. Given the likely integration of generative AI tools such as large language models (e.g., ChatGPT) or other general-purpose AI or foundational models into downstream products, how can AI accountability mechanisms inform people about how such tools are operating and/or whether the tools comply with standards for trustworthy AI?

---

[17] UNESCO Recommendation on the Ethics of AI 2021, https://unesdoc.unesco.org/ark:/48223/pf0000377897

CAIDP has filed a complaint[18] with the Federal Trade Commission (FTC) against OpenAI extensively documenting the verifiable harms of generative AI tools built on large-language-models. The FTC has issued Guidelines for AI-based businesses and/or commercial products. The 2020 FTC statement on *Using Artificial Intelligence and Algorithm[19]*, the 2021 FTC statement on *Statement Aiming for Truth, Fairness, and Equity in Your Company's use of AI[20]* and the 2023 FTC statement on *Keep your AI claims in check[21]* point towards two key aspects of accountability: truthful and honest representation supported by "verifiable substantiation"[22] and "doing more good than harm".

If accountability mechanisms like independent impact assessments reveal that AI systems do not function as intended or promised, produce discriminatory outcomes, fail to respect privacy, are opaque and foundationally flawed they should not be deployed or if deployed, should be discontinued, or corrected. Providers and/or regulators of such systems should have a duty to inform the public of such outcomes.

B. *Existing Resources and Models (Response to Question 9)*

9. What AI accountability mechanisms are currently being used? Are the accountability frameworks of certain sectors, industries, or market participants especially mature as compared to others? Which industry, civil society, or governmental accountability instruments, guidelines, or policies are most appropriate for implementation and operationalization at scale in the United States? Who are the people currently doing AI accountability work?

We reiterate that guidance should be taken from existing governance frameworks - the Universal Guidelines for AI and the OECD AI Principles for establishing assurance and assessment mechanisms.

Accountability mechanisms in the U.S could be based on the EU AI Act considering the global nature of the technologies and the desirability of ensuring interoperable assurance across jurisdictions. The EU AI Act[23] identifies high-risk AI systems such as systems that

---

[18] In the Matter of OpenAI, https://www.caidp.org/cases/openai/

[19] Andrew Smith, Director, FTC Bureau of Consumer Protection, *Using Artificial Intelligence and Algorithms*, (April 8, 2020), https://www.ftc.gov/business-guidance/blog/2020/04/using-artificial-intelligence-and-algorithms

[20] FTC, *Aiming for truth, fairness, and equity in your company's use of AI* (April 2021) (emphasis below in the original), https://www.ftc.gov/business-guidance/blog/2021/04/aiming-truth-fairness-equity-your-companys-use-ai

[21] FTC, *Keep your AI claims in check* (February 2023), https://www.ftc.gov/business-guidance/blog/2023/02/keep- your-ai-claims-check

[22] Remarks of Commissioner Rebecca Kelly Slaughter Algorithms and Economic Justice, UCLA School of Law, (January 24, 2020), https://www.ftc.gov/system/files/documents/public_statements/1564883/remarks_of_commissioner_rebecca_kelly_s laughter_on_algorithmic_and_economic_justice_01-24-2020.pdf

[23] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT)

make decisions related to health or insurance eligibility, voting and election campaigns, and systems that interact with children. The EU AI Act requires providers to register their use of high-risk AI systems and sets out a certification process under which providers will obtain a certification number. The following accountability policies from the EU AI Act could be adopted in the U.S.:

- **Identifying high-risk systems,** AI systems that adversely impact fundamental rights (right to non-discrimination, freedom of expression, human dignity, privacy) should be classified as high-risk.

- **Mandatory Ex-Ante human rights impact assessments**, pre-deployment and throughout the AI lifecycle. There should be mandatory ex-ante human rights impact assessments as well as a requirement for AI systems providers to document impact of large AI systems (especially training systems) on the environment, emission, and waste.

- **Disclosure and filing requirements,** upstream and downstream providers of AI systems and public as well as private entities deploying AI systems should be required to disclose and file their impact assessments with a centralized agency or sector specific regulators.

- **Accountability by design,** should be ensured through examination of, for example, bias in model design. Selection of performance metrics should systematically be considered and AI system decision error rates across protected categories under a fundamental rights/human rights impact assessment should be transparent, made publicly available, along with a statement from the Provider as to why that error rate was an acceptable level for the AI system to be put into market.

- **Third-Party/Independent Certification, Audit requirements and technical standards** should be mandated as a part of accountability measures. The standard setting process should include broad-based participation of civil society and public interest organizations to ensure that commercial interests do not dominate the standard setting process of accountability mechanisms. The practice of U.S. Food and Drug Administration (pre-market approvals) and/or the Securities and Exchange Commission (pre-IPO due diligence) are illustrative and established agency processes which can be examined when designing accountability mechanisms for AI systems providers.

AND AMENDING CERTAIN UNION LEGISLATIVE ACTS, COM/2021/206 final, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206

- **Complaint mechanisms,** accountability systems should establish a complaint and redress mechanism for impacted individuals or groups to challenge AI systems that breach health, safety, and fundamental rights

C. *Accountability Subjects (Response to Question 16)*

16. The lifecycle of any given AI system or component also presents distinct junctures for assessment, audit, and other measures. For example, in the case of bias, it has been shown that ''[b]ias is prevalent in the assumptions about which data should be used, what AI models should be developed, where the AI system should be placed—or if AI is required at all.'' How should AI accountability mechanisms consider the AI lifecycle?

All AI actors across the lifecycle, are responsible for the transparent and fair design, development, deployment, and use of AI systems, according to their role. **We believe that the key to effective AI accountability is to allocate rights and responsibilities for AI developers and users.** This allocation will necessarily be asymmetric as those who are designing the big models are far more able to control outcomes and minimize risk than those who will be subject to the outputs.[24] We reiterate that regulation must start where the control is most concentrated.

General purpose AI systems can encode biases that determine the fairness and accuracy of downstream applications.[25] A foundation model trained on medical data, for example, may inherit the existing disparities and inequalities in healthcare access and quality across different regions or populations, leading to discriminatory or harmful outcomes. Assigning liability to upstream actors is likely to incentivize these actors to ensure the quality, safety, and robustness of their foundation models and to monitor and mitigate possible biases and harms.[26] It could also provide more accountability and transparency for the users and applications downstream.

D. *Accountability Inputs and Transparency (Response to Question 20)*

20. What sorts of records (e.g., logs, versions, model selection, data selection) and other documentation should developers and deployers of AI systems keep in order to support AI accountability? How long should this documentation be retained? Are there design principles (including technical design) for AI systems that would foster accountability-by-design?

---

[24] M. Rotenberg, *A Turning Point for U.S. AI Policy: Senate Explores Solutions,* (May 17, 2023), *https://cacm.acm.org/blogs/blog-cacm/273011-a-turning-point-for-us-ai-policy-senate-explores-solutions/fulltext*

[25] R. Bommasani, *On the opportunities and risks of foundation models* (July 2022), https://arxiv.org/pdf/2108.07258v1.pdf.

[26] P. Hacker, *Regulating ChatGPT and other large generative AI models* (May 2023), https://arxiv.org/abs/2302.02337.

It is necessary to ensure data access to conduct audits and assessments prior to deployment and during the lifecycle of AI systems including the following:

- **Training data:** The data that the AI system was trained on should be assessed for the system's potential biases, accuracy, and robustness. Inspecting training data can reveal whether the system has been trained on data that is representative and ethically sourced. However, due to privacy concerns, direct access to the raw training data might not always be possible. Techniques like Differential Privacy could be employed to address these concerns.

- **Model parameters:** Access to the models' weights and architecture might be necessary, especially for deep learning systems. Though interpreting these parameters can be challenging, they can help in understanding the systems' complexity and potential susceptibility to overfitting or underfitting. With regard to generative AI systems based on large-language-models (LLMs) it is recommended that disclosure should include "*thorough documentation on the data used in model building, including the motivations underlying data selection and collection processes. This documentation should reflect and indicate researchers' goals, values, and motivations in assembling data and creating a given model.*"[27]

- **Testing and validation data:** This data, along with performance metrics, can give a sense of how well the AI system performs on unseen data and help in the assessment of its generalizability.

- **Output data:** Data about the systems' predictions or decisions, and their consequences, can help in assessing the AI systems' real-world impact.

- **Documentation:** Details about the systems' purpose, design, expected behavior, handling of data, and any steps taken to ensure fairness, privacy, and robustness can provide critical context for the audit. The documentation should be dynamic to reflect changes to data, model, and performance in real-time.

E. *Barriers to Effective Accountability (Response to Question 25, 26)*

25. Is the lack of a general federal data protection or privacy law a barrier to effective AI accountability?

---

[27] Emily M. Bender, Timnit Gebru, Angelina McMillan-Major, Margaret Mitchell, *On the Dangers of Stochastic Parrots: Can Language Models Be Too Big*, FAccT '21: Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency (March 2021). Pages 610, 615, 618 https://doi.org/10.1145/3442188.3445922

We have explained above (See, Response to Question #9) that AI safeguards build on data protection law.[28] The absence of a federal privacy legislation is a barrier to effective AI accountability. As we explained in ***AI and Democratic Values***, following our review of AI policies and practices in the United States, "*The absence of a legal framework to implement AI safeguards and a federal agency to safeguard privacy also raises concerns about the ability of the U.S. to monitor AI practices.*"[29]

26. Is the lack of a federal law focused on AI systems a barrier to effective AI accountability?

In March, CAIDP President Merve Hickok testified before the US Congress on "Advances in AI: Are we ready for the tech revolution." Ms. Hickok told Members of Congress, "No, we do not have the guardrails in place, the laws that we need, the public education, or the expertise in government to manage the consequences of the rapid changes that are now taking place."[30] We reiterate our recommendation for a federal law on AI to ensure effective accountability of AI systems. Voluntary frameworks such as NIST's RMF do not ensure accountability, which is critical given the individual and collective risks posed by unregulated AI systems.

We also reiterate our recommendations for comprehensive regulations for AI used by federal agencies. CAIDP supports many of the principles set out in the Guidance for Regulation of Artificial Intelligence Applications, issued by the OMB in November 2020, particularly regarding public trust, public participation, transparency, safety, and fairness and non-discrimination.[31] It is time, however, to move beyond principles. Executive Order 139604 and the AI in Government Act of 20205 make clear that the OMB now has a legal obligation to seek public comment and establish regulations for the development and deployment of AI techniques by federal agencies. The OMB should issue the government-wide memorandum and begin the formal rulemaking for the regulation of AI, as required by E.O. 13960 and the AI in Government Act.[32][33]

---

[28] See also Marc Rotenberg, *Foreword: Artificial Intelligence and Democratic Values: The Role of Data Protection,* European Data Protection Law Review (Winter 2021), https://edpl.lexxion.eu/article/EDPL/2021/4/6

[29] CAIDP, *Artificial Intelligence and Democratic Values Report,* at 1085, https://www.caidp.org/reports/

[30] Testimony of Merve Hickok before the House Oversight Committee, "Advances in AI: Are We Ready for the Tech Revolution?" March 8, 2023, https://oversight.house.gov/wp-content/uploads/2023/03/Merve-Hickok_testimony_March-8th-2023.pdf

[31] OMB, Guidance for Regulation of Artificial Intelligence Applications (Nov. 17, 2020), https://www.whitehouse.gov/wp-content/uploads/2020/11/M-21-06.pdf

[32] CAIDP Statement to the US Office of Management and Budget on the Need to Establish Regulations for the Use of AI by Federal Agencies (Oct. 19, 2021). https://www.caidp.org/app/download/8350420263/CAIDP-OMB-Statement-19102021.pdf

[33] CAIDP Statement to the US Office of Management and Budget. CAIDP Renews Call to OMB to Initiate AI Rulemaking (Apr. 24 2023). https://www.caidp.org/app/download/8454950563/CAIDP-Statement-OMB-04242023.pdf

Center for AI and
Digital Policy

F. *AI Accountability Policies (Response to Question 34)*

34. Is it important that there be uniformity of AI accountability requirements and/or practices across the United States? Across global jurisdictions? If so, is it important only within a sector or across sectors? What is the best way to achieve it? Alternatively, is harmonization or interoperability sufficient and what is the best way to achieve that?

We recommend baseline safeguards for AI Accountability. States should be encouraged to develop innovative AI accountability measures as new challenges emerge. We offer the following recommendations on accountability measures.

- **Require scientific validity:** If an AI system is not scientifically valid, it should be prohibited. This requirement should be added to existing requirements for accuracy, representativeness, robustness, and cybersecurity. **Predictive policing, Emotion recognition and Biometric categorization systems do not have scientific validity.** As such AI Accountability systems should be designed in a manner to prevent creation of such systems pre-deployment and, if detected at the later stage of the AI lifecycle, should prohibit further deployment.[34]

- **Require ex-ante human rights impact assessments:** Providers of high-risk systems in should be obligated to conduct ex-ante 'human rights impact assessment'. The results of the assessment should be included in the documentation submitted to a centralized database and should be publicly accessible.[35]

- **Require User Registries:** Providers of high-risk AI systems and both public and private users of these systems should be required to register in a central database accessible by federal agencies charged with enforcement of accountability obligations. Such registration should correspond to the certification identification number of the Provider. Without such transparency, it will be impossible for individuals, disadvantaged groups, and market monitoring authorities like the FTC to understand the impact, prevalence, and current status of the particular system in use.

- **Record Serious Incidents:** There should be a process of reporting serious incidents corresponding to the certification identification number of the Provider.

- **Mandate Independent, third-party auditing:** High-risk AI systems should be subject to audit and such audit should be completed within a mandated timeline.

---

[34] CAIDP, *Statement on the EU Council's General Approach on the EU Artificial Intelligence Act,* (Feb. 2023), https://www.caidp.org/resources/eu-ai-act/
[35] *Id.*

- **Establish obligation to terminate AI system no longer under human control:** Where high-risk AI systems generate unacceptable risks to fundamental rights, or if human control of the system is no longer possible, Providers and Users should have an affirmative obligation to terminate the system. As such, the kill-switches should be a key design requirement for high-risk AI systems.

We support the NTIA   ks for ensuring accountability of AI systems. T   .
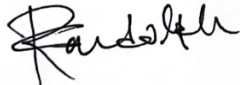
We would welcome   her about these recommendations.

Marc Rotenberg
CAIDP Executive Director

Merve Hi
CAIDP President

Christabel Randolph
Law Fellow

Sunny Gandhi
CAIDP Research Assistant

Damilola Awotula
CAIDP Research Assistant