July 7, 2023

Office of Science and Technology Policy
Executive Office of the President
Eisenhower Executive Office Building
1650 Pennsylvania Avenue, NW
Washington, D.C. 20504
AI-Strategy@ostp.eop.gov

Via regulations.gov portal and email

Re: Request for Information on National AI Strategy (FR Doc. 2023–11346)

Dear Office of Science and Technology Policy:

On behalf of the Software & Information Industry Association (SIIA), we write in response to the request for information on National Priorities for Artificial Intelligence (RFI) issued by the Office of Science and Technology Policy (OSTP). SIIA appreciates OSTP's continued attention to advancing responsible innovation in artificial intelligence (AI) and its efforts to develop a comprehensive, whole-of-society approach to harness the potential and mitigate the risks of AI technologies.

SIIA is the principal trade association for the software and digital information industries. Our members include over 450 companies reflecting the broad and diverse landscape of digital content providers and users in academic publishing, education technology, and financial information, along with creators of software and platforms used by millions worldwide, and companies specializing in data analytics and information services. As the only association representing both those who develop and deploy these engines and those who create the information that feeds environments, SIIA is uniquely positioned to provide insight on AI accountability and innovation and provide recommendations for the direction of U.S. policy that advances a values-based approach to AI-related risks and opportunities.

SIIA has long supported efforts by the federal government to advance proactive AI policy efforts.[1] We have called for use-based guardrails and tailored requirements for those AI systems that are likely to carry the highest risk to safety and rights. Since at least 2016, we have made clear that a host of existing laws apply equally to uses of AI as to other activities but that gaps remain that require attention to address AI accountability. Throughout, we have stressed the importance of viewing innovation and governance as complementary, rather than oppositional goals. Fostering trustworthy and responsible AI

[1] *See, e.g.,* SIIA, Submission to NTIA on AI Accountability (Jun. 12, 2023) (https://www.siia.net/wp-content/uploads/2023/06/SIIA-Response-to-NTIA-on-AI-Accountability-Policy.pdf); SIIA, Comments on Artificial Intelligence Export Competitiveness Submitted to the International Trade Association (Oct. 17, 2022) (https://www.siia.net/wp-content/uploads/2022/10/SIIA-Comments-to-ITA-2022-0007.pdf); SIIA, Comments on Study to Advance a More Productive Tech Economy Submitted to NIST (Feb. 14, 2022) (https://www.siia.net/wp-content/uploads/2022/02/SIIA-Submission-for-NIST-Emerging-Tech-Study.pdf); SIIA, Comments on Public and Private Sector Uses of Biometric Technologies Submitted to OSTP (Jan. 14, 2022) (https://www.siia.net/wp-content/uploads/2022/01/SIIA-Submission-on-OSTP-Biometrics-RFI.pdf); SIIA, "Ethical Principles for Artificial Intelligence and Data Analytics" (Sept. 15, 2017); SIIA, "Algorithmic Fairness" (Sept. 22, 2016).

through measures that are tailored to the risks of AI systems will benefit U.S. innovation as a whole and raise the profile of the United States as a global leader.

1. **What specific measures – such as standards, regulations, investments, and improved trust and safety practices – are needed to ensure that AI systems are designed, developed, and deployed in a manner that protects people's rights and safety? Which specific entities should develop and implement these measures?**

Design, development, and deployment of AI systems in a manner that protects rights and safety – what we refer to generally as responsible and trustworthy AI – requires a mix of measures - some underway, some yet to develop. We appreciate how OSTP has framed this question as we believe there is no single approach to advancing responsible and trustworthy AI.

As a starting point, we believe all AI systems should conform with best practices for testing, evaluation, validation, and verification (TEVV) across the AI lifecycle.[2] The practices will necessarily differ for different types of systems and based on their intended application. In general, however, these practices include documentation, risk assessments, and transparency measures, where appropriate, in a manner that protects trade secrets and other intellectual property. Accountability measures improve the performance of AI systems, empower their users, and help to establish trust in AI systems designed to address key needs across our society.

While adoption of best practices is not automatic, we are seeing increased attention to responsible AI development and deployment; that is a direct consequence of growing attention to the potential and risks of AI in the past three years.[3] Some of this is industry driven. Indeed, many of SIIA's members at the forefront of AI have been leaders in advancing AI accountability and governance.[4] The reason is simple: AI that generates the most accurate information, limits unintentional bias, and builds on reliable data will be most useful to governments, businesses, and consumers. SIIA members have developed internal governance and systems oversight procedures to advance accountability and mitigate the potential for unintended bias and other risks.

Likewise, continued efforts of the National Institute of Standards and Technology (NIST) and international technical standardization are critical. The NIST AI RMF reflects the most comprehensive framework by the U.S. government (and perhaps anywhere in the world) for identifying, assessing, and mitigating risks. It is the culmination of a multi-stakeholder, expert-driven, and transparent 18-month

---

[2] *See* NIST, Artificial Intelligence Risk Management Framework (AI RMF 1.0), NIST AI 100-1 (Jan. 2023), at 9-10 (https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf).

[3] A robust literature on trustworthy and responsible AI has developed in the past several years as public, private, and academic research has proliferated. This literature provides a rich toolbox of systems and governance solutions to advance AI accountability. We are particularly pleased to see deep engagement by government agencies, including OSTP and NIST – discussed later in this submission - and others, including the Government Accountability Office (GAO). *See, e.g.,* GAO, "Artificial Intelligence: An Accountability Framework for Federal Agencies and Other Entities," GAO–21–519SP (June 30, 2021) (https://www.gao.gov/products/gao-21-519sp.pdf).

[4] *See, e.g.,* Google, "A Policy Agenda for Responsible Progress in Artificial Intelligence" (May 2023) (https://storage.googleapis.com/gweb-uniblog-publish-prod/do); Meta, "Facebook's five pillars of Responsible AI" (June 2021) (https://ai.facebook.com/blog/facebooks-five-pillars-of-responsible-ai/); RELX, "Responsible Artificial Intelligence Principles at RELX" (relx-responsible-ai-principles-0622.pdf); Adobe, "Adobe's Commitment to AI Ethics" (https://www.adobe.com/content/dam/cc/en/ai-ethics/pdfs/Adobe-AI-Ethics-Principles.pdf).

process. The RMF, the NIST AI Roadmap, and other resources at NIST's Trustworthy & Responsible AI Center provide guidance on AI accountability measures. The value of these resources will only increase as NIST finalizes AI RMF Profiles based on key use cases.[5] Also critical is the development of international technical standards on AI.[6]

For most AI systems, SIIA believes self-assessments and increased transparency measures will provide the necessary accountability while avoiding undue burden on innovation and small and midsize businesses. Development of a voluntary code of conduct could be a productive way to ensure that all entities in the private sector agree to baseline standards for AI accountability. Further in this submission (*see* question 3), we provide recommendations on a more active government oversight role for high-risk systems and use cases and recommend entities within the U.S. government to be involved in these processes.

2. **How can the principles and practices for identifying and mitigating risks from AI, as outlined in the Blueprint for an AI Bill of Rights and the AI Risk Management Framework, be leveraged most effectively to tackle harms posed by the development and use of specific types of AI systems, such as large language models?**

We recommend that the National AI Strategy lean heavily on the NIST AI RMF project as a foundation for its guidance on trustworthy and responsible AI. This includes developing methods to mitigate risks and harms associated with the development of AI systems; aligning definitions and taxonomy for policymaking across the federal government;[7] and looking to NIST—as a non-regulatory agency grounded in science, expertise, and non-partisanship—as a focal point for collaboration working closely with academia, civil society, and industry to develop best practices for AI risk mitigation.

The OSTP Blueprint for an AI Bill of Rights (the Blueprint) should continue to serve as a guidepost and vision statement regarding the potential impacts that AI systems can have on civil rights.[8] We view

[5] NIST, Trustworthy & Responsible AI Resource Center, "AI RMF Profiles" (https://airc.nist.gov/AI_RMF_Knowledge_Base/AI_RMF/Core_And_Profiles/6-sec-profile).

[6] Among these is the work of Subcommittee 42 (SC 42) of Joint Technical Committee 1 of the International Organization for Standardization/International Electrotechnical Commission. SC 42 has been a focal point of international standardization in the areas of accountability, data quality, and governance, and will issue Standard 42001 on AI system management later this year. *See* ISO/IEC JTC 1/SC 42, Artificial Intelligence Standards (https://www.iso.org/committee/6794475/x/catalogue/p/0/u/1/w/0/d/0). SC 42 is among several international technical standards organizations pursuing aligned approaches for AI management. In addition, organizations like the General Partnership on AI (https://gpai.ai/) are critical to advancing alignment reflecting multi-stakeholder approaches that will inform domestic and international alignment on AI development and use.

[7] In addition to those definitions that NIST has advanced in the AI RMF, we commend an ongoing effort to align definitions with the European Union to reflect "shared technical, socio-technical and values-based understanding of AI systems." *See* U.S.-EU Trade & Technology Council, "EU-U.S. Terminology and Taxonomy for Artificial Intelligence," 1st Ed. (May 31, 2023) (https://digital-strategy.ec.europa.eu/en/library/eu-us-terminology-and-taxonomy-artificial-intelligence).

[8] White House Office of Science and Technology Policy, "Blueprint for an AI Bill of Rights" (Oct. 2022) (https://www.whitehouse.gov/wp-content/uploads/2022/10/Blueprint-for-an-AI-Bill-of-Rights.pdf).

the Blueprint as a statement of principles across several domains that will grow in operational impact as designated agencies, such as the Department of Education, issue concrete guidance to stakeholders.

Both the NIST AI RMF and OSTP Blueprint are relevant to identify and mitigate risks associated with foundation models, including large language models (LLMs). We support efforts to apply these frameworks to foundation models in the design and development phases.[9] However, given the countless uses of foundation models and the wide availability globally of several LLMs (including well over two dozen open-source LLMs), we recommend that any formal restrictions or regulations focus in a targeted manner on concerning uses of foundation models rather than on their development.[10]

3. **Are there forms of voluntary or mandatory oversight of AI systems that would help mitigate risk? Can inspiration be drawn from analogous or instructive models of risk management in other sectors, such as laws and policies that promote oversight through registration, incentives, certification, or licensing?**

We believe there is limited utility in attempting to develop a framework for AI governance that draws heavily from regulatory frameworks used in other contexts. While well-established oversight frameworks for financial services, and pharmaceutical safety, for example, provide some appeal, we believe the multiple uses of AI technologies call for a *sui generis* approach. AI is being incorporated into products and services across the economy in every sector and by a wide range of public and private actors. This calls for a different approach to mitigating risk.

There is a growing consensus in the United States and the global AI policy community to pursue a risk-based approach to AI governance. Such an approach will focus limited public resources, minimize compliance costs—especially on small and medium-sized businesses—and avoid stifling innovation. There is, however, no one-size-fits-all solution to address these systems and uses. Oversight and accountability measures should be grounded in the types of AI systems and should be proportionate to the potential risks associated with each system or the intended uses of those systems.

For most AI systems, we encourage voluntary measures. Industry standards and norms, public and expert scrutiny, market dynamics, and government policy guidance have significant value in raising the bar on oversight and governance. It is critical for even low-risk AI systems to be developed and used responsibly. Yet vague, overbroad, or unnecessarily burdensome regulations will inevitably hinder AI firms from innovating and render them incapable of keeping pace with foreign competitors, prevent small and midsize firms from competing with large technology companies, and hurt the ability of Americans to access technology that may positively impact their daily lives.

For high-risk systems, and high-risk uses of AI systems, we encourage the U.S. government to take steps to develop and implement guardrails that go beyond best practices. To start with, we recommend the U.S. government adopt a uniform definition of "high risk" that would be calibrated, as described below, by agencies with the expertise and experience to oversee high risk systems and uses in different sectors. Google recently proposed a definition that we view as a good starting point: "Define

[9] *See, e.g.,* https://fas.org/publication/how-do-openais-efforts-to-make-gpt-4-safer-stack-up-against-the-nist-ai-risk-management-framework/

[10] This approach has been suggested by IBM. *See* Christina Montgomery, Francesca Rossi, Joshua New, IBM, "A Policymaker's Guide to Foundation Models" (May 1, 2023) (https://newsroom.ibm.com/Whitepaper-A-Policymakers-Guide-to-Foundation-Models). IBM is not a member of SIIA.

'high-risk systems' as those intended for use in applications that pose a material risk of significantly harming people or property or imperiling access to essential services."[11]

We further recommend that the National AI Strategy endorse a sector-based approach that delegates to the appropriate agencies the authority to identify the right mix of accountability measures that should apply to high-risk AI systems in those domains. Accountability measures must be tailored to the specific AI systems at issue and the intended uses of those systems. This requires an understanding of how technology is and can be used in diverse sectors, as well as expertise to undertake necessary oversight activities. In addition, it is the experts within each sector who can best provide tailored guidelines to determine which systems used in that sector should be considered high risk. Indeed, not every use of AI in the educational context will meet the definition of high-risk, even if as a general matter education is one of several areas that warrant extra care.[12]

To identify relevant agencies, ewe recommend looking to the focus categories identified in the OSTP Blueprint, which highlights employment, education, housing, access to financial services, and criminal justice, as well several bills introduced in Congress during the past two sessions, which highlight those areas as well as essential utilities, transportation, public benefits, and immigration.[13]

Several U.S. agencies have already begun to carry out exactly this sort of approach to AI accountability. The Food and Drug Administration (FDA) currently undertakes a regulatory review of AI/ML-enabled medical devices and requires that those devices be reviewed and authorized before they can be marketed.[14] The Federal Reserve, as the RFC notes, along with other financial regulators, have provided guidance on financial institutions' use of AI.[15] The Equal Employment Opportunity Commission (EEOC) is undertaking a process to provide accountability requirements to mitigate the potential for AI-based discrimination and bias.[16] And recently, the Department of Education issued recommendations on

---

[11] Google, "A Policy Agenda for Responsible Progress in Artificial Intelligence" (May 2023), at 10 (https://storage.googleapis.com/gweb-uniblog-publish-prod/do).

[12] *See* SIIA and European EdTech Alliance, Letter to B. Benifei and D. Tudorache (Feb. 9, 2023) (https://www.siia.net/wp-content/uploads/2023/02/SIIA-and-EEA-Letter-on-EU-AI-Act-9-Feb-2023.pdf).

[e]) (identifying as a "critical decision" one that "meaningfully affects access to, or the cost, terms, or availability of" educational and vocational training, employment, essential utilities, transportation, public benefits, financial services, asylum and immigration services, healthcare, and housing).

[14] U.S. Food & Drug Admin., "Software as a Medical Device" (https://www.fda.gov/medical-devices/digital-health-center-excellence/software-medical-device-samd).

[15] See Board of Governors of the Federal Reserve System, Supervisory Guidance on Model Risk Management, Federal Reserve SR Letter 11–7 (Apr. 4, 2011) (https://www.federalreserve.gov/supervisionreg/srletters/sr1107.htm); *see also* U.S. Dept. of Treasury, Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, Bureau of Consumer Financial Protection, and National Credit Union Administration, Request for Information and Comment on Financial Institutions' Use of Artificial Intelligence, Including Machine Learning, 86 FR 16837 (Mar. 31, 2021) (https://www.govinfo.gov/content/pkg/FR-2021-03-31/pdf/2021-06607.pdf).

[16] U.S. Dept. of Justice, Consumer Financial Protection Board, Federal Trade Comm., EEOC, "Joint Statement on Enforcement Efforts Against Discrimination and Bias in Automated Systems" (Apr. 25, 2023) (https://www.ftc.gov/system/files/ftc_gov/pdf/EEOC-CRT-FTC-CFPB-AI-Joint-Statement%28final%29.pdf).

the use of AI for education and teaching.[17] Of these, the FDA model provides perhaps the most robust process to date for government oversight of high-risk AI systems.

We recommend increased attention to and expansion on this sector-based work for high-risk systems. AI accountability measures must be tailored to the AI systems at issue, focused on how those systems will be used and the risks attendant with use of systems in particular contexts. Agencies with oversight and regulatory responsibility for sectors most likely to involve high-risk AI systems should take the lead on identifying the appropriate accountability mechanisms. Balancing interests of transparency, accuracy, privacy, protection of individual rights, trade secret protection, and security will be essential to fashion the right approach to accountability – and it's the agencies closest to the AI systems' uses that will be best positioned to identify the goals to balance.

Agencies should also undertake an assessment of whether there is a need for targeted use-based restrictions relating to high-risk AI systems. Such an assessment should evaluate the need for additional authorities, if any, to develop rules to guide how high-risk AI systems may be used. We are encouraged by the ongoing NIST effort to create AI Profiles by sector and use and believe this effort will be instructive in identifying sectors most likely to have high-risk AI systems that warrant more proactive government guidance or action.

In addition, we recommend that the U.S. government identify an appropriate office or agency to oversee and coordinate activity across the Executive Branch. We recommend that this function be embedded in the National Artificial Intelligence Initiative Office (NAIIO), or shared with the Office of Management and Budget. NAIIO is best positioned to coordinate across federal agencies, address cross-cutting matters, provide guidance on implementing Administration policy, and liaise with the private sector and civil society. We are concerned that NAIIO is not sufficiently resourced to carry out this oversight function. We encourage the Administration to ensure that NAIIO has adequate funding and staff to lead U.S. government efforts on AI accountability.

4. What are the national security benefits associated with AI? What can be done to maximize those benefits?

AI has the potential to revolutionize the tools and methods of national security in myriad ways, from intelligence analysis, to supply chain security, to military logistics and safety. We refer OSTP to excellent work undertaken by the National Security Commission on Artificial Intelligence (NSCAI) and successor efforts of the Special Competitive Studies Project.[18]

7. What are the national security risks associated with AI? What can be done to mitigate these risks?

AI technologies have extraordinary potential to advance the values and institutions of democratic societies. Yet these technologies have no inherent normative disposition and can be, and

[17] U.S. Dept. of Education, Office of Educational Technology, "Artificial Intelligence and the Future of Teaching and Learning" (May 2023) (https://www2.ed.gov/documents/ai-report/ai-report.pdf).

[18] *See generally* National Security Commission on Artificial Intelligence, "Final Report" (Mar. 2021) (https://www.nscai.gov/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf); Special Competitive Studies Project, "Mid-Decade Challenges to National Competitiveness" (Sep. 2022) (https://www.scsp.ai/wp-content/uploads/2022/09/SCSP-Mid-Decade-Challenges-to-National-Competitiveness.pdf).

have been, deployed by state and non-state actors to advance anti-democratic objectives including social control, unlawful surveillance, social destabilization, and dissemination of disinformation. SIIA is dedicated to the health of the information ecosystem and the advancement of productive uses of information. Anti-democratic uses of AI technologies are anathema not only to democratic society at large but also to our members' businesses.

The work of NSCAI and countless thought leaders, academics, members of Congress, and government officials has demonstrated the scope of national security risks associated with AI. SIIA believes the administration has made significant strides to address certain these risks through export controls, enhancements to investment screening procedures, policy alignment with allies and partners, legislation designed to advance AI adoption across the national security enterprise, redoubled attention on international technical standardization activities, and digital development initiatives at USAID.

An additional way to mitigate the national security risks associated with AI is to reimagine how the government engages with industry (and other non-government actors in civil society and academia) to promote values-based innovation in and global standards for emerging technologies. As noted above, while AI policy has innovation, responsible actors in the private sector have led on developing accountability measures, mitigating AI-associated risks, and pioneering state of the art compliance measures. These actors, who develop and deploy AI technologies in the United States and abroad, can be important ambassadors to mitigate against national security risks associated with unsafe and unsecure technologies and AI used to undermine core democratic values.

We provide recommendations on national security risks associated with AI-enabled disinformation and deepfakes in response to question 15.

9. What are the opportunities for AI to enhance equity and how can these be fostered? For example, what are the potential benefits for AI in enabling broadened prosperity, expanding economic and educational opportunity, increasing access to services, and advancing civil rights?

SIIA is a firm believer that accessible education leads to a more equitable society. AI, if implemented correctly, can expand the opportunities of individuals through education and workforce. We believe that the deployment of AI in education must be done in a way that empowers economic growth associated with the development and use of these tools. In the field of education, digital equity must be of the utmost importance, so that members of society can utilize the AI tools to enhance their desired career pursuit. The Department of Education's recent AI report specifically addresses the issue of equity, as it states the definition of digital equity from their Advancing Digital Equity report[19], stating: "the condition in which individuals and communities have the information technology capacity that is needed for full participation in the society and economy of the United States." For AI to increase possibilities in the economic market, digital equity must be addressed, so that there is elevated access to the tools. We believe that an equitable use of AI-systems in the market is essential.

Many members of SIIA have already fostered AI tools that contribute to the success of the economy. From autofill text, to assistive chatbots - companies are able to reach more individuals in the marketplace, thus fostering growth and engagement in the American economy. We have collected

[19] U.S. Dept. of Education, Office of Educational Technology, "Advancing Digital Equity for All" (Sept. 2022) (https://tech.ed.gov/files/2022/09/DEER-Resource-Guide_FINAL.pdf).

several examples of these AI applications in "ANNEX: Socially Beneficial AI Innovation by SIIA Member Companies," attached to this submission.[20]

10. What are the unique considerations for understanding the impacts of AI systems on underserved communities and particular groups, such as minors and people with disabilities? Are there additional considerations and safeguards that are important for preventing barriers to using these systems and protecting the rights and safety of these groups?

Due to rapid advancements in AI models and data labeling, the diversity of populations that this technology can assist is expected to increase by the day. AI has the potential to create numerous opportunities for marginalized populations, specifically with education, health, and the workforce. In the field of education, the optimism is high as it relates to students with disabilities, English learners, and underserved populations. Specifically, as mentioned in the Department of Education's Office of Education Technology AI report, it states "[m]any educators are actively exploring AI tools as they are newly released to the public. AI tools should treat each person fairly and actively work to prevent unintended bias and unjust impacts on people. Educators see opportunities to use AI-powered capabilities like speech recognition to increase the support available to students with disabilities, multilingual learners, and others who could benefit from greater."[21] However, as AI technology continues to advance, it is imperative that its implementation takes into account learner variability and abides by current laws and policies that align with existing frameworks established by state and federal laws - including privacy, accessibility, and other important civil rights laws. Furthermore, it is important to recognize that AI tools must be designed to perform in an equitable manner, ensuring that bias and discrimination is eliminated as algorithms progress.

11. How can the United States work with international partners, including low- and middle-income countries, to ensure that AI advances democratic values and to ensure that potential harms from AI do not disproportionately fall on global populations that have been historically underserved?

The United States should prioritize efforts to seek cross-border alignment on AI governance to the extent such alignment furthers core U.S. and democratic values. SIIA has in the past recommended that officials in the United States and other countries develop guiding principles or standards to implement risk-based approaches to AI systems. These would explicitly build on the substantial work already undertaken on accountability to include measures around safety, security, trustworthiness, and bias.[22] Harmonization of requirements across jurisdictions will aid not only innovation in general but also the advancement of concrete guidelines for values-based AI. We are supportive of work underway at the OECD, within the TTC, as part of the G7's new Hiroshima Process, and through international standards

---

[20] *See also* SIIA, "Case Study: Empowering Educators with Innovative AI-Based Assessment Solutions: A Look Into Cambium Assessment" (Jul. 2023) (https://www.siia.net/wp-content/uploads/2023/07/Case-Study-Cambium-Assessment-Incorporated.pdf); SIIA, "Case Study: Data as Their Superpower: How 5 Companies Used Data for Good" (Jan. 2022) (https://www.siia.net/wp-content/uploads/2022/01/Final-Case-Study-_-Jan-2022-SIIA.pdf).

[21] U.S. Dept. of Education, Office of Educational Technology, "Artificial Intelligence and the Future of Teaching and Learning" (May 2023) (https://www2.ed.gov/documents/ai-report/ai-report.pdf).

[22] *See, e.g.,* SIIA, Comments on Artificial Intelligence Export Competitiveness Submitted to the International Trade Association (Oct. 17, 2022) (https://www.siia.net/wp-content/uploads/2022/10/SIIA-Comments-to-ITA-2022-0007.pdf).

efforts such as SC 42. We recommend that OSTP encourage this work to continue with a focus on high-risk systems in core areas. This will require greater resourcing and policy attention in key agencies, especially the Department of State and Commerce, and coordination across the interagency. It will also require greater attention—and funding—for the digital development efforts of USAID. As these efforts continue, we further recommend increased engagement with non-governmental stakeholders about international AI policy and foreign AI regulation potentially through a new advisory committee focused on this topic.

13. How might existing laws and policies be updated to account for inequitable impacts from AI systems? For example, how might existing laws and policies be updated to account for the use of generative AI to create and disseminate non-consensual, sexualized content?

The United States has a robust legal framework for addressing potential inequitable impacts from AI systems. These include federal sectoral privacy laws and state sectoral and comprehensive privacy laws, anti-discrimination laws, and others that take technology-neutral approaches - meaning they apply equally to actions taken by humans or enabled by AI or other technologies. For example, Title VII is technology-neutral, as is the Fairness in Lending Act and other authorities.[23] Employment discrimination and redlining remain illegal. Credit bureaus are required to maintain "maximum possible accuracy," and will be using AI to maintain it. Nonetheless, the government will need both internal expertise and external cooperation to understand and guide the development and deployment of AI systems under existing law. And where the technology's use clearly presents a unique and unmistakable obstacle to longstanding policy goals, additional regulation may be appropriate.

With respect to generative AI, SIIA strongly recommends that the United States enact a comprehensive federal privacy law. SIIA and its members have advocated strongly for federal privacy legislation for years and are active in engaging with members of Congress and administrations of both parties. A federal privacy bill is the number one solution to closing the gaps on the use of personal data and data-driven technologies and driving innovation in the U.S. economy. Currently, the patchwork of state laws across the nation create uncertainty for consumers and businesses, burden companies with duplicative compliance costs (estimated at $1 trillion over 10 years) and have a disproportionate impact on growth and innovation for small- and medium-sized businesses.[24] This will grow as additional states pass privacy legislation – unless Congress acts first. Domestically, the benefits of a federal privacy regime include creating baseline harmonization of consumer and business expectations surrounding personal information; supporting and fueling further competitive innovation in emerging technologies; and more deeply embedding diversity, equity and inclusion into privacy, emerging tech, and AI policies and practices. We are at a unique moment politically when bipartisan support seems achievable, and a federal privacy bill provides a vehicle to provide redress for individuals who have been harmed by the dissemination of non-consensual, sexualized content.

15. What are the key challenges posed to democracy by AI systems? How should the United States address the challenges that AI-generated content poses to the information ecosystem, education, electoral process, participatory policymaking, and other key aspects of democracy?

---

[23] *See generally* SIIA, "Algorithmic Fairness" (Sept. 22, 2016) at 8-9 (https://history.siia.net/Portals/0/pdf/Policy/Algorithmic%20Fairness%20Issue%20Brief.pdf).

[24] *See* Information Technology & Industry Foundation, The Looming Cost of a Patchwork of State Privacy Laws (Jan. 24, 2022).

Maintaining a trustworthy digital ecosystem, one that addresses growing and malign influence efforts, is important for the health of the internet and entire digital ecosystem. Disinformation can erode social cohesion and human rights,[25] with a disproportionate effect on marginalized communities.[26] AI supercharges the ability of state and non-state actors to spread disinformation creating a systemic risk for the entire information environment.[27] Synthetic media, including deepfakes, provide a special challenge because of how they deliberately distort existing images, video, and audio.[28]

Advancing tools that the public can rely on to determine credibility of information sources is particularly important. Credibility labels, flagging tools, and content provenance specifications are among the methods that the government should encourage. We are encouraged by the work of the Coalition for Content Provenance and Authenticity, which has developed technical specifications to certify the provenance of media content.[29] This builds on work of several private firms, including one of our member companies, Adobe.[30] This is a core area where further efforts within the U.S. government and between the government and private firms would be extremely beneficial. In the last Congress, we supported the Deepfake Task Force Act[31] as providing a foundation for essential coordination to address deepfakes. Since that time, the advent of generative AI tools widely available to the public (and to malicious state and non-state actors) has increased, adding urgency to the challenge.

In addition, we would encourage the U.S. government, through the intelligence community, to take an active role in publicly prebunking and debunking widely disseminated disinformation intended to destabilize democratic processes. While this presents challenges, an authoritative voice can help to break through in an increasingly noisy environment.

Lastly, we call for greater support for digital literacy and civic education across the United States. Overall, federal government investment in digital literacy and civic education has decreased substantially in recent years. Student scores on the Nation's Report Card for civics and history have declined in the past two decades. The number of online platforms with different approaches to content moderation has

---

[25] Carme Colomina, et al., The impact of disinformation on democratic processes and human rights in the world, European Parliament (April 2021).

[26] Center for Democracy and Technology, Facts and their Discontents: A Research Agenda for Online Disinformation, Race, and Gender (2021).

[27] *See, e.g.,* Katerina Sedova, et al., Georgetown Center for Security and Emerging Technology, AI and the Future of Disinformation Campaigns (Dec. 2021).

[28] Kartik Hosanagar, Deepfake Technology Is Now a Threat to Everyone. What Do We Do?,Wall Street Journal (Dec. 7, 2021); Tim Hwang, Georgetown Center for Security and Emerging Technology, Deepfakes: A Grounded Threat Assessment (July 2020).

[29] Coalition for Content Provenance and Authenticity, C2PA Specifications.

[30] Eric Abent, Adobe Expands Content Authenticity Initiative Tools to Fight Misinformation, SlashGear.com (Oct. 26, 2021).

[31] S.2559, Deepfakes Task Force Act (117th Cong.); U.S. Senate Comm. on Homeland Security & Govt. Affairs, Tech Leaders Support Portman's Bipartisan Deepfake Task Force Act to Create Task Force at DHS to Combat Deepfakes (July 30, 2021).

proliferated alongside the rise of AI in the past several years. In today's internet and AI-driven society, both digital literacy and civic education are strategic imperatives.[32] Teaching skills to help students become astute purveyors of the rapidly changing information ecosystem and responsible citizens should be a bipartisan priority, and one essential to further America's shared values in the AI age. This will require funding and renewed policy efforts.

17. **What will the principal benefits of AI be for the people of the United States? How can the United States best capture the benefits of AI across the economy, in domains such as education, health, and transportation? How can AI be harnessed to improve consumer access to and reduce costs associated with products and services? How can AI be used to increase competition and lower barriers to entry across the economy?**

SIIA believes that AI tools can contribute to key aspects of the American economy. Specifically in education, AI can assist with tutoring, teaching methods, and chatbot/digital assistance tools. A report curated by UNESCO contributes to the conversation by stating, that "[t]he use of AI technologies…aim to provide every learner, wherever they are in the world, with access to high-quality, personalized, and ubiquitous lifelong learning."[33] AI tools can also assist with relieving teachers from many activities that could be considered "time-consuming." Further, in a recent report released by the U.S. Department of Education's Office of Education Technology, it states "[e]ducators see opportunities to use AI-powered capabilities like speech recognition to increase the support available to students with disabilities, multilingual learners, and others who could benefit from greater adaptivity and personalization in digital tools for learning.[34]

18. **How can the United States harness AI to improve the productivity and capabilities of American workers, while mitigating harmful impacts on workers?**

SIIA believes that engaging the working population in the advancement of AI is essential. It is imperative that AI is strategically curated to be more of an assistance to the workforce than a replacement so that the American workforce is strong, inventive and up-to-speed. Yet, the U.S. should invest in AI digital literacy so that the workforces can critically examine its presence and determine its role and value in their own lives and careers.

For many careers, AI can provide additional assistance and solutions to their workload, as well as reduce burnout. We encourage the government to support innovation for AI in work and labor by increasing development of resources and opportunities.

---

[32] *See, e.g.,* Center for Strategic & International Studies, "The Digital Literacy Imperative" (July 2022) (https://www.csis.org/analysis/digital-literacy-imperative); Center for Strategic & International Studies, "Civics as a National Security Imperative" (https://www.csis.org/programs/international-security-program/defending-democratic-institutions/civics/civics-national). *See also* National Commission on Military, National, and Public Service, "Inspired to Serve" (Mar. 2020), at 13-21 (https://www.sss.gov/wp-content/uploads/2022/08/Final-Report-National-Commission.pdf).

[33] United Nations Educational, Scientific and Cultural Organization, "AI and education: Guidance for policy-makers" (2021) (https://unesdoc.unesco.org/ark:/48223/pf0000376709).

[34] U.S. Dept. of Education, Office of Educational Technology, "Artificial Intelligence and the Future of Teaching and Learning" (May 2023) (https://www2.ed.gov/documents/ai-report/ai-report.pdf).

19. What specific measures – such as sector-specific policies, standards, and regulations – are needed to promote innovation, economic growth, competition, job creation, and a beneficial integration of advanced AI systems into everyday life for all Americans? Which specific entities should develop and implement these measures?

Further to the issue of resourcing, SIIA believes the United States cannot continue to be a leader in responsible AI without providing the necessary resources to support responsible innovation and advance the state of the art on AI accountability. We encourage the government to support innovation in AI accountability by increasing funding for important initiatives. This includes funding NIST, the Department of Energy's Science Division, and the National Science Foundation in accordance with the programs authorized in the CHIPS and Science Act. It also includes ensuring that NIST has adequate funds to continue to advance its work on the AI RMF. In addition, we encourage the government to fully fund the programs set out in the National AI Research Resource (NAIRR) Task Force report issued earlier this year.[35] The NAIRR can be a transformational vehicle for advancing U.S. AI innovation in a way that democratizes access to compute and data. The government can also lead the way in creating AI accountability certification programs to train personnel to augment the federal workforce.

23. How can the United States ensure adequate competition in the marketplace for advanced AI systems?

AI has the potential to bring fundamental changes to key aspects of how we live, and how governments and businesses operate. This is true, for example, in healthcare, logistics, and transportation.[36] But it is also one of the main drivers of democratized access to technology and innovation, allowing companies large and small to automate routine processes and to quickly analyze mind-numbing amounts of data, just as it can help them develop new products and services.

While the use of AI is proliferating, market dynamics are working well. Further cementing a vibrant and competitive AI ecosystem, however, will require the active and collaborative participation of not just governmental entities but also the private sector and civil society. Among the elements that are needed to leverage the promise of AI are the availability of and access to copious amounts of data, a workforce with the requisite skill sets, including engineering and machine learning, the ability of companies to quickly find, hire, and train them, and broad access to the computational resources, often delivered through the cloud, to take full advantage of the immense opportunities it offers. For the U.S. to continue to lead in AI and tech more broadly, it is important for public and private sectors to work collaboratively to implement programs for citizens to develop the requisite skills, build and maintain the necessary physical and technological infrastructure, and continue to invest in research and development in order to continue to lead in the race to innovate new AI models, algorithms, and other new technologies.

---

[35] National Artificial Intelligence Research Resource Task Force, "Strengthening and Democratizing the U.S. Artificial Intelligence Innovation Ecosystem" (Jan. 2023) (https://www.ai.gov/wp-content/uploads/2023/01/NAIRR-TF-Final-Report-2023).

[36] Niklas Bergland, et al., McKinsey & Company, "The Potential Value of AI—and how governments could look to capture it" (July 2022) (https://www.mckinsey.com/industries/public-sector/our-insights/the-potential-value-of-ai-and-how-governments-could-look-to-capture-it).

29. Do you have any other comments that you would like to provide to inform the National AI Strategy that are not covered by the questions above?

We recommend that the National AI Strategy include a plan for advancing the adoption of privacy enhancing technologies (PETs) in government and in the private sector. PETs refer to a category of technologies that enable productive uses of information while ensuring protection of data confidentiality, as required by applicable law. Indeed, a combination of new legal frameworks (in the United States and globally) combined with advances in "big data" and AI have driven the need to consider PETs alongside the broader category of AI technologies. SIIA has been vocal in advocating for policy measures to advance PET adoption.[37] At a minimum, the National AI Strategy should incorporate recommendations contained in the National Strategy to Advance Privacy-Preserving Data Sharing and Analytics[38] and address how PETs can be used to mitigate risks associated with AI and enable productive uses of information generated through AI systems.

* * *

SIIA thanks OSTP for the opportunity to provide input on the National AI Strategy. We look forward to continuing to work with OSTP on this important endeavor.

Sincerely,

Paul Lekas
Senior Vice President, Global Public Policy & Government Affairs
Software & Information Industry Association

[37] *See, e.g.,* SIIA, Comments on RFI on Advancing Privacy-Enhancing Technologies (Aug. 2022) (https://2540091.fs1.hubspotusercontent-na1.net/hubfs/2540091/SIIA%20Response%20to%20PETs%20RFI%20-%20081222.pdf).

[38] National Science and Technology Council, "National Strategy to Advance Privacy-Preserving Data Sharing and Analytics" (Mar. 2023) (https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Strategy-to-Advance-Privacy-Preserving-Data-Sharing-and-Analytics.pdf).

ANNEX: Socially Beneficial AI Innovation by SIIA Member Companies

SIIA's members are engaged in developing and using AI for myriad socially beneficial purposes. This chart provides examples of some of those AI tools. It is not intended to be exhaustive of the socially beneficial initiatives undertaken by SIIA's membership as a whole or by the companies identified in the chart.

Company	Examples of Socially Beneficial AI Tools
Amazon	• Helping non-profits to achieve their missions and enable socially beneficial outcomes in sustainability, accessibility, and civil rights
Apple	• Using AI to help with accessibility for users with disabilities
Cambium Assessment	• Empowering educators with AI-based assessment solutions • Using AI to identify at-risk student responses to tests
D2L	• Using AI to discover opportunities and mitigate risks in career planning
Enveil	• Human trafficking detection • Encryption with machine learning • Unlocking analysis of health data in a privacy-protective manner
GoGuardian	• Using AI to filter content harmful to students
Google	• Google AI and Social Good (various) • Diabetic retinopathy screening • Forecasting riverine floods • Helping people with non-standard speech be better understood • Speech-based reading tutor app • AI to prepare for and adapt to effects of rising heat
Meta	• Meta AI Blog (various) • Data for Good initiatives (various) • Automated fairness indicators for computer vision
Pearson	• Personalized training for language learners
Refinitiv/LSEG	• Tracking indicia of financial crime
RELX	• Using AI to help smaller legal firms • Finding missing children
Thomson Reuters	• Helping knowledge workers find information faster • Solving cold cases
Turnitin	• AI detection to combat plagiarism