Submission of the Software & Information Industry Association in Response to the Office of Management and Budget's Request for Comments on *Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence* Memorandum

Federal Register Docket 2023-24269

December 5, 2023

On behalf of the Software & Information Industry Association (SIIA), we appreciate the opportunity to provide input on the Office of Management and Budget's (OMB) draft memorandum, *Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence* (the "Draft AI Memo"). The Executive Order on Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence (the "AI Executive Order") will have a significant impact in promoting development and adoption of responsible AI in the United States and influence the direction of AI policy globally in a manner that supports democratic values. We are pleased to see the thorough approach OMB has taken in the Draft AI Memo and hope the comments we provide in this submission will prove helpful as OMB refines its guidance.

Introduction

SIIA is the principal trade association for the software and digital information industries. Our members include nearly 400 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 measures for the government's responsible adoption of AI and procedures designed to advance 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

[1] *See, e.g.,* SIIA, *Blueprint for Government Oversight and Regulation of AI* (July 2023) (https://www.siia.net/wp-content/uploads/2023/07/Blueprint-for-Government-Oversight-and-Regulation-of-AI.FINAL-1.pdf); 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) (https://history.siia.net/Portals/0/pdf/Policy/Ethical%20Principles%20for%20Artificial%20Intelligence%20and%20D

that are likely to carry the highest risk to safety and rights. Throughout, we have stressed the importance of viewing innovation and governance as complementary, rather than oppositional goals. Most recently, in October, SIIA released *The Education Technology Industry's Principles for the Future of AI in Education*.[2] These principles intend to specifically guide the education technology (ed tech) industry as the broader education community continues toward deploying these impactful technologies. Fostering trustworthy and responsible AI 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.

SIIA is pleased that OMB recognizes the need for practical solutions that help improve outcomes and experiences of the advancement of AI. Many of SIIA's members at the forefront of AI have been leaders in advancing AI accountability and governance.[3] 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. As the trade association dedicated to the information side of "information technology," SIIA applauds OMB's approach to removing barriers to AI adoption to advance government use of AI. For the U.S. to continue to lead in AI and tech more broadly, it is important for the public and private sectors to join in the shared goal of helping citizens develop the requisite skills, build and maintain the necessary physical and technological infrastructure, and continue to invest in research and development to position the United States at the forefront of responsible innovation.

The accountability measures called for by the Draft AI Memo will, overall, 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. Our recommendations are designed to help to focus government resources, advance responsible adoption of AI, and mitigate harm to individuals.

---

ata%20Analytics%20SIIA%20Issue%20Brief.pdf?ver=2017-11-06-160346-990); SIIA, *Algorithmic Fairness* (Sept. 22, 2016) (https://history.siia.net/Portals/0/pdf/Policy/Algorithmic%20Fairness%20Issue%20Brief.pdf).

[2] SIIA, *Education Technology Industry's Principles for the Future of AI in Education* (October 2023) (https://edtechprinciples.com/)

[3] *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); SIIA, *Education Technology Industry's Principles for the Future of AI in Education* (October 2023) (https://edtechprinciples.com/)

Responses to OMB Questions

1. The composition of Federal agencies varies significantly in ways that will shape the way they approach governance. An overarching Federal policy must account for differences in an agency's size, organization, budget, mission, organic AI talent, and more. Are the roles, responsibilities, seniority, position, and reporting structures outlined for Chief AI Officers sufficiently flexible and achievable for the breadth of covered agencies?

SIIA commends OMB for developing detailed guidance for the new Chief AI Officer (CAIO) functions, including roles and responsibilities, and we believe the framework contained in the Draft AI Memo provides sufficient flexibility for covered agencies to implement AI practices required by the AI Executive Order. Building the infrastructure necessary to effectively scope, adopt, and implement AI tools to meet critical government needs is a herculean task and will require dedicated leadership and lines of effort.

That task must be borne not just by the public sector but the private sector as well. Accordingly, information about the CAIOs and their backgrounds should be part of the public profiles of agency leadership provided online, as it will help align hiring processes across public and private sector, similar to what the Workforce Framework for Cybersecurity (the NICE Framework) has done for cybersecurity. This will also help keep the public informed while ensuring agencies consider how other roles, such as their CDO, CIO, or CISO will interact with the CAIOs, especially as it is such a cross-cutting technology. As we discuss in response to question 2, we recommend further attention to interagency infrastructure that can be leveraged by multiple agencies to provide governance, technical guidance, and technical support to help agencies achieve their objectives.

We have some concern that the minimum practices for safety-impacting and rights-impacting AI along with the additional minimum practices for rights-impacting AI will impede effective and timely adoption of AI by all agencies. We discuss this in more detail in response to questions 5 and 6. Though the Draft AI Memo would permit CAIOs to seek waivers as needed, it begins with the presumption that the minimum and additional minimum practices should be undertaken.

Given funding and human resource constraints, we recommend that OMB consider an approach that is better tailored to the risk profiles of the categories of safety-impacting and rights-impacting AI set out in Section 5.b.i and Section 5.b.ii. Rather than treating all rights-impacting AI in the same way, for example, OMB could treat certain of the minimum or additional minimum practices as recommended but not required – flipping the presumption – depending on the level of risk attendant to the use. As noted below, we recommend following the NIST AI Risk Management Framework for making such determinations.

It is critical that the government balances AI safety and the protection of rights against the governmental interests in adopting AI to achieve significant government objectives. Recognizing this balance, and incorporating it into the agency guidance, we believe will help to achieve a framework that fulfills the vision of the AI Executive Order.

2. What types of coordination mechanisms, either in the public or private sector, would be particularly effective for agencies to model in their establishment of an AI Governance Body? What are the benefits or drawbacks to having agencies establishing a new body to perform AI governance versus updating the scope of an existing group (for example, agency bodies focused on privacy, IT, or data)?

SIIA has been a leading proponent of strong interagency coordination on AI governance and accountability.[4] This is critical to leverage limited resources and advance consistency on common issues. OMB or another entity within EOP – such as the Office of Science and Technology Policy or the National AI Initiatives Office – seems best situated to handle functions around coordinating AI governance across agencies. We further recommend additional funding to NIST to undertake the necessary steps to build consistency around the NIST AI Risk Management Framework and related standards for impact assessments and other requirements – those set out in the minimum and additional minimum practices.

In addition, we recommend OMB consider centralized processes to undertake additional functions. First, it should build technical expertise to assist in the many pre-deployment and ongoing monitoring obligations, ideally in a manner that can be leveraged by multiple agencies to avoid duplication of effort and benefit from economies of scale. To do this, OMB may look to the 18F and United States Digital Service as models for creating technological expertise to provides services across the government. Second, it should coordinate the necessary outreach with non-governmental actors, including the private sector and civil society, will be necessary. We can envision situations in which the necessary coordination becomes overwhelming for some agencies; a streamlined, coordinated approach will help to conserve resources.

Within agencies themselves, there may be existing governance bodies or boards that can be leveraged, especially if they are resourced appropriately. Where a 1:1 fit does not exist, gaps should account for those existing bodies to ensure optimal coordination mechanisms are put in place. Among those coordination mechanisms, the importance of transparency via public meetings, opportunities to provide feedback, and comment periods for significant policy updates or changes will not only maintain the critical trust-building approach to integrating AI

[4] SIIA, *Blueprint for Government Oversight and Regulation of AI* (July 2023) (https://www.siia.net/wp-content/uploads/2023/07/Blueprint-for-Government-Oversight-and-Regulation-of-AI.FINAL-1.pdf).

into the public sector but also allow the government to obtain the benefits that come from such public-private partnerships.

The cybersecurity domain provides a good model of effective interagency and intra-agency coordination and coordination with non-governmental actors. We recommend that OMB consider modeling this effort on the mechanisms and programs that the Cybersecurity and Infrastructure Security Agency (CISA) has spearheaded.

3. How can OMB best advance responsible AI innovation?

OMB has a critical role in advancing responsible AI innovation both as a coordinator of administration and interagency priorities and as a liaison with Congress. In this response, we provide a handful of suggestions.

First, OMB can advocate for necessary resources for agencies to undertake new and augmented responsibilities required under the AI Executive Order and OMB's own guidance. While in some cases agencies may have necessary authorities and funding, in other cases appropriations from Congress may be required. Devising ways to create economies of scale across the interagency and build technical expertise will require OMB's leadership.

Second, OMB can prioritize efforts to fund research and development programs, including those authorized (but not funded) under the CHIPS and Science Act, and ensure that NIST, the National Science Foundation, and the Department of Energy's Science Division have requisite funds to advance responsible AI innovation. We also encourage OMB to pursue establishment and funding of programs set out in the National AI Research Resource (NAIRR) Task Force report issued earlier this year, including supporting passage of the CREATE AI Act.

Third, OMB has an important role in advancing responsible AI innovation in the education space. This is a priority for SIIA's membership given our significant work with companies across the ed tech ecosystem and involvement in a range of projects to advance responsible adoption of AI in education. 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.

The education community is optimistic about the positive impact AI can have in the learning journeys of all students and, in particular, students with disabilities, English learners, and underserved populations. The U.S. Department of Education's (ED) recent report explains "[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."[5] From tutoring and test preparation to assessing learner performance to relatively simple tasks like checking the spelling and grammar of a document, AI technologies are and can have a great impact on teaching and learning. [6] Because of this and in order to realize AI's promise, stakeholders must address and embrace ways to encourage the safe innovation of these technologies.

SIIA believes that the successful deployment of AI technologies in education must be done in a way that supports those who use it, protects innovation in the field, and addresses the risks associated with the development and use of these new tools. AI should replace neither the educator nor the learning experience. As mentioned before, SIIA released The *Education Technology Industry's Principles for the Future of AI in Education*, which builds on experiences with and successes in using AI technologies to advance educational objectives. These principles provide a framework for how we can look to the future of implementing AI technologies in a purpose-driven, transparent, and equitable manner. These principles intend to guide the ed tech industry as the broader education community continues toward deploying these impactful technologies.

Fourth, OMB should promote, where appropriate, sector-specific guidelines developed with expert stakeholders. For example, currently, the leadership and staff at ED have taken on the important task of directly engaging with a large number of stakeholders to build out useful resources for practitioners and the broader education community like ed tech vendors, teachers, school leadership, parents, and students.

Fifth, OMB should encourage agencies to highlight the importance of using and moving to an interoperable and open public commercial cloud architecture that can support a multi-cloud environment that leverages existing investments in on-premises and government clouds to achieve the promise and security of AI.

If America wants to be the leader in AI innovation, then we believe that we must commit to develop responsible and trustworthy technologies focused on ensuring all products are purpose-driven, privacy-focused, explainable, equitable, reliable, and accountable.

---

[5] U.S. Department 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).

[6] AI in education refers to the tools used in teaching and learning inside and outside the four walls of a classroom. AI technologies may be used in the development or deployment of software used in an educational setting but are not part of the teaching and learning experience.

5. Are there use cases for presumed safety-impacting and rights-impacting AI (Section 5 (b)) that should be included, removed, or revised? If so, why?

We recommend that OMB focus the use cases for safety-impacting and rights-impacting AI and provide agencies with further guidance that will promote consistency across the federal government, avoid overbreadth, and promote continuity across future administrations.

Focus Definitions of Safety-Impacting and Rights-Impacting AI on High-Risk AI.

As an initial matter, we strongly agree with the risk-based approach that OMB has endorsed in the Draft AI Memo. However, we recommend refinement to the definitions of safety-impacting and rights-impacting to promote certainty and avoid inadvertently capturing a variety of low risk activities. For example, while the use cases for rights-impacting AI[7] align with categories where high-risk applications of AI are likely to be found, there are use cases within each category that will not present the same risk profile with regard to individual rights and privileges, including equitable access, access to services, and so on.

To better approximate a risk-based approach, we recommend refining the definitions of safety-impacting and rights-impacting AI. We recommend limiting safety-impacting AI systems to those that pose a risk of loss of human life or serious physical injury. We recommend focusing rights-impacting AI systems to exclude circumstances where an AI system is incidental or accessory to making the consequential decision. Rights-impacting AI should be scoped to decisions that are already regulated by existing laws, such as non-discrimination or consumer protection, to ensure clarity around the type of activity regulated in this circumstance.

Ensure Consistency between Rights-Impacting AI Definition and Use Cases.

The Draft AI Memo defines "rights-impacting AI" as "AI whose output serves as a basis for decision or action that has a legal, material, or similarly significant effect" on a variety of rights and privileges.[8] We appreciate the effort to enumerate AI applications that are presumptively rights-impacting in Section 5.b.ii. Section 5.b.ii, however, contains language different than that used in the definition of rights-impacting AI to guide agencies in their classification of AI. There, AI is deemed to be rights-impacting "if it is used to control or meaningfully influence the outcomes of any of the [enumerated] activities or decisions."[9] It is not clear from this whether the standard in Section 5.b.ii is meant to augment or limit the standard contained in the

[7] Office of Management and Budget, Draft AI Mem. Section 5.b.ii.

[8] Office of Management and Budget, Draft AI Mem. Section 6 (at page 24).

[9] Office of Management and Budget, Draft AI Mem. Section 5.b.ii.

definition of rights-impacting AI. Read by itself, the Section 5.b.ii standard is broader than the definitional standard, but read conjunctively would function to refine the definition.

We recommend that OMB refine this language to provide further consistency to agencies and to providers of AI used by the government and to more tightly scope the definitions associated with safety- and rights-impacting AI. Effectively, as it currently stands, OMB is defining virtually all applications as high-risk in ways that will make it difficult or impossible for federal agencies to adopt AI tools. Notably, the EU's AI Act, while generally embracing a category-based approach, does define "high risk" applications subject to heightened review more narrowly than the Draft AI Memo. This is important because the classification of an AI system as rights-impacting triggers the additional minimum requirements set forth in the Draft AI Memo. We also note a similar disjunction is present in the definition of safety-impacting AI and the list of use cases in Section 5.b.i.

Narrow Rights-Impacting AI Use Cases on High-Risk Examples.

We appreciate the thoughtful approach taken in the Draft AI Memo to identify categories of AI use cases that are presumptively rights-impacting. As a general matter, we would recommend that OMB require agencies to conduct a risk assessment to determine whether particular use cases should adhere to the additional minimum requirements of rights-impacting AI. To achieve this, we recommend that OMB explicitly require agencies to apply a risk-assessment that follows the NIST AI Risk Management Framework when determining which AI applications within the different use case categories should be treated as rights-impacting AI under the definition of that term.[10]

Additionally, it is worth reiterating that the definitions of both safety- and rights-impacting AI are broad enough that they could disincentivize the government from adopting AI in positive instances. This chilling effect could discourage the adoption of new technologies that serve diverse users, including those that would spread benefits to overburdened and underserved communities.

In addition to this overarching comment, we provide the following suggestions for refinement of the use cases of rights-impacting AI set out in Section 5.b.ii to assist OMB in providing more precise guidance to agencies.

- *Section 5.b.ii.A. Decisions to block, remove, hide, or limit the reach of protected speech;*

Online content moderation outside of the government domain has for years relied on a combination of human and machine learning processes to make determinations about user-generated content that comports with content policies. While the First Amendment provides

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

robust protection for these practices in the private sector, the First Amendment limits the federal government's discretion to block, remove, hide, or limit the reach of protected speech. We support the inclusion of this set of use cases as presumptively risk-impacting insofar as the intent is to limit its scope to government-run websites or platforms.

- *Section 5.b.ii.B. Law enforcement or surveillance-related risk assessments about individuals, criminal recidivism prediction, offender prediction, predicting perpetrators' identities, victim prediction, crime forecasting, license plate readers, iris matching, facial matching, facial sketching, genetic facial reconstruction, social media monitoring, prison monitoring, forensic analysis, forensic genetics, the conduct of cyber intrusions, physical location-monitoring devices, or decisions related to sentencing, parole, supervised release, probation, bail, pretrial release, or pretrial detention;*

We agree with OMB that the use of AI tools for law enforcement or surveillance-related risk assessments represents an area that is presumptively high-risk and rights-impacting. However, the description of this category captures a wide variety of potential government actions. It is not clear what is and is not included, and there is a good chance that this language will be interpreted to cover a number of otherwise low-risk AI applications. Given that, adhering to the additional minimum practices in Section 5.c.v would have the effect of impeding effective and responsible adoption of AI systems for critical governmental purposes without meaningfully adding to the protection of individuals' rights and privileges. Moreover, these seem to go beyond the scope of the AI Executive Order, which calls for the identification of "areas where AI can enhance law enforcement efficiency and accuracy, consistent with protections for privacy, civil rights, and civil liberties."[11]

We suggest the following clarifications to this category: First, disambiguate between law enforcement and surveillance-related risk assessments. While law enforcement has a well understood meaning, "surveillance-related risk assessments" could apply to anything from law enforcement to FDA inspections. The scope of surveillance-related risk assessments is not clear outside the law enforcement context and could be interpreted in different ways. Second, focus the category on those law enforcement purposes that have a direct impact on individuals' rights. Third, limit the recourse mechanisms - notification to negatively affected individuals and opt-out rights – when doing so would jeopardize important government ends such as the need to maintain confidentiality in an open investigation and is not required by the Constitution or applicable law. Fourth, consider clarification about the use case involving "the conduct of cyber intrusions."

[11] White House AI Exec. Order Section 7.1(b)(ii)(A).

- *Section 5.b.ii.C. Deciding immigration, asylum, or detention status; providing risk assessments about individuals who intend to travel to, or have already entered, the U.S. or its territories; determining border access or access to Federal immigration related services through biometrics (e.g., facial matching) or other means (e.g., monitoring of social media or protected online speech); translating official communication to an individual in an immigration, asylum, detention, or border context; or immigration, asylum, or detention-related physical location monitoring devices.*

Similar to the law enforcement context, the use of AI tools in immigration is presumptively high-risk and rights-impacting but also presents a variety of use cases where some of the additional minimum steps could unreasonably impede governmental objectives. Facial matching–which we read to mean authentication and/or verification using facial recognition technology–presents significantly less risk than do other uses of facial recognition technology - or than many of the other uses contained in this category. While safeguards are required to ensure the AI tools deliver as promised, some of the additional minimum steps could impede responsible adoption. In general, we recommend this set of use cases be further delineated in accordance with a risk-based assessment.

- *Section 5.b.ii.D. Detecting or measuring emotions, thought, or deception in humans;*

This category stands out from the others in that it is not tied to a particular field of activity. We suggest clarifying the areas in which this may arise to give agencies and the public additional guidance.

- *Section 5.b.ii.E. In education, detecting student cheating or plagiarism, influencing admissions processes, monitoring students online or in virtual-reality, projecting student progress or outcomes, recommending disciplinary interventions, determining access to educational resources or programs, determining eligibility for student aid, or facilitating surveillance (whether online or in-person);*

SIIA and the ed tech industry recognize the need to manage the risk of AI used in the field of education. The Draft AI Memo defines "safety-impacting AI" as AI that has the potential to meaningfully impact, among other things "human life or well-being, including loss of life, serious injuries, bodily harm, biological or chemical harms, occupational hazards, harassment or abuse, or mental health, including both individual and community aspects of these harms." Further, OMB's definition for "rights-impacting AI" includes impacts on an individual's "civil rights, civil liberties, or privacy, including but not limited to freedom of speech, voting, human autonomy, and protections from discrimination, excessive punishment, and unlawful surveillance."

We recognize the sensitivity around the use of AI systems in the educational context. We concur with the spirit of OMB's guidance thereto about the importance of ensuring that AI systems used in the educational context are properly designed, do not foster discrimination, and contain

safeguards to protect citizens' rights at all levels. We believe, however, that subjecting all AI systems used in the educational context to the additional minimum requirements for "rights-impacting AI" could impair the ability to use these tools to advance learning objectives, if not defined clearly.

Based on the proposed guidance, it seems that OMB has virtually captured many different uses of AI in the education context within the scope of rights-impacting AI. We believe that the deployment of AI in education must be done in a way that addresses specific risks associated with the development and use of these tools and is appropriately tailored to cover high-risk applications. However, we must point out that in the field of education, the AI tools and their reach/impact in education can have completely different effects. With the diversity of AI-based platforms, as shown above, the draft guidance will need to provide more clarity into what "rights" are impacted in education, as many different types of rights may be affected within different scenarios. For example, plagiarism might impact a "right to intellectual property," where surveillance might impact "right to privacy." Are the rights equivalent? Could they be treated the same? Designating all AI systems used in the educational context as "riskier" will subject the field of ed tech to a plethora of rules and regulations, which allows the agency to "prove" that their AI-based system is trustworthy and meets the mandatory requirements.

Furthermore, in education, we encourage OMB to consider the evolving policy landscape of existing regulations, in addition to new policy developments on the horizon, when it comes to AI in education. Ed tech vendors and educational institutions already have legal and ethical obligations to protect students online through a range of data privacy laws, including CIPA, FERPA and COPPA. OMB should consider the additional compliance methods already set in place in these areas, and consider exempting from the list of presumptively "high-risk" use cases those which education agencies are undertaking specifically to comply with statutory obligations. Our members believe that it is important that OMB's guidance on responsibly integrating AI into federal agencies' work compliments, rather than complicates current education industry requirements.

AI presents an opportunity for schools to fulfill their obligation to better implement content filtering and to deploy technology in a way that, with the right guardrails in place, improves student safety. As mentioned above, CIPA already imposes certain requirements on schools or libraries that receive discounts for internet access or internal connections through the Federal Communications Commission's (FCC) E-Rate program. To receive E-Rate funding, schools are required to certify that they have internet safety policies in place that include technology protection measures against content that is obscene, pornographic, or harmful to minors. There are also certification requirements under CIPA that require schools to have internet safety policies that monitor the online activity of minors.

Furthermore, survey research confirms that parents and educators worry deeply about children's online activity and overwhelmingly support technology protections on school-issued devices to keep kids from accessing harmful content. For example, in a July 2022 survey of more

than 2,400 public school educators and parents, 80 percent of parents and 88 percent of teachers agreed that unrestricted access to the internet on school-issued devices can be detrimental to student mental health.[12] In the same survey, 89 percent of parents and 93 percent of teachers agreed that if there were an online tool that could detect signs that a student may be at risk of harming themselves, then this technology should be deployed on a school-issued device. When implemented properly, AI can help schools achieve these broadly supported safety objectives.

Although we all agree on the importance of the safety and efficacy of AI systems in the education market, we still believe the approach of "grouping" different types of AI tools in ed tech will offer some challenges to the field the field of education, if OMB does not review the complexity of what constitutes a "right" and how differently the rights can impact AI tools within the field of education.

- *Section 5.b.ii.J. Decisions regarding access to, eligibility for, or revocation of government benefits or services; allowing or denying access—through biometrics or other means (e.g., signature matching)—to IT systems for accessing services for benefits; detecting fraud; assigning penalties in the context of government benefits;*

The government interest in detecting fraud is significant and is one where certain of the additional minimum requirements around redress – notification to negatively affected individuals and opt-out rights – would undermine governmental objectives. In addition, we recommend limiting this category to those decisions to deny access rather than decisions that also allow access to programs and systems.

6. Do the minimum practices identified for safety-impacting and rights-impacting AI set an appropriate baseline that is applicable across all agencies and all such uses of AI? How can the minimum practices be improved, recognizing that agencies will need to apply context-specific risk mitigations in addition to what is listed?

As a general matter, SIIA recommends that responsibility for impact assessment performance evaluation and ongoing monitoring lie with the system deployer rather than developer because the deployer is closer to the intended use cases. In addition, we note that several of the practices would require agencies to conduct assessments and undertake monitoring in areas where traditionally they have not had the kind of expertise or access that the Draft AI Memo

[12] Morning Consult, *EdTech in Schools: Creating Safer Digital Learning Environments* (July 2022) (https://uploadsssl.webflow.com/60db82d1be38ad3341c2ff23/6324e2698b87f308a5085bc3_Edtech%20in%20Schools%20-%20Creating%20Safer%20Digital%20Learning%20Environments.pdf)

contemplates. Agencies, with OMB's leadership, should focus on up-skilling their existing workforce in order to meet the needs of enhanced AI procedures.

Furthermore, with the existing definitions being even broader than those present in the EU's AI Act, a large swath of AI use cases will be subject to these minimum practices, many of which are not the type to cause the risk of harm the memo is concerned with. In fact, this is likely to create enough complexity and red tape to harm the speed and breadth of adoption that would help the government fulfill the promise of this technology.

Comments on Minimum Practices for Safety- and Rights-Impacting AI.

The minimum practices will require a significant amount of government resources, given the breadth of the safety-impacting and rights-impacting AI enumerated in Section 5.b. We caution that the resource requirements – specifically, the requirement to test the AI for performance in a real-world context and the requirement to independently evaluate the AI – may impede effective adoption of responsible AI to advance significant government objectives. To that end, we would encourage OMB to incorporate a risk-based assessment within both categories and identify those requirements that are required of only the highest-risk AI systems within each.

In addition to a risk-based approach, we recommend tailoring requirements for rights-impacting AI to reflect the existing legal frameworks that already provide important risk mitigation to AI tools. Education provides an excellent case study in this. As AI technologies continue to advance, it is imperative that the implementation takes into account product variability and purposes and that a specific product in education aligns 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.

When considering "minimum practices" for education, one must ensure that the recommendations are practical and create a complimentary impact instead of a disparate impact. Given the growing awareness and attention to the dangers children might encounter online, SIIA encourages the federal government to consider the evolving policy landscape of existing regulations, in addition to new policy developments on the horizon, when it comes to AI in education and the practices it must follow.

In addition, as noted above in our discussion of the categories of rights-impacting AI, we believe some of the additional minimum practices will on balance impede the responsible adoption of AI without adding meaningful safeguards to affected individuals. SIIA would like OMB to reassess the possible burdens of the specific practices required of the two types of AI systems:

- *Independently evaluate the AI:* We believe that this practice will be extremely burdensome on the agencies. 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 agencies.

- *Mitigate emerging risks to rights and safety:* We believe that this is key, however, we have a concern that this requirement is too broad when defining the word "risk." We implore OMB to further define the word "risk," specifically "emerging risks" that are related to security, privacy, and data protection.

We also encourage OMB to reexamine the requirements regarding the quality and appropriateness of the relevant data that is part of the pre-deployment AI impact assessment. In many cases, assessment of training data will be unhelpful to assess AI system performance and, likely, prove a poor investment of resources that could be spent focusing on how an AI system performs in real-world testing environments. In addition, agencies are unlikely to have access to the training data in a way that would allow for the contemplated analyses - in part for practical reasons, and in part because of the need to protect IP and proprietary data.

Related to the latter point, we encourage OMB to include provisions that would permit agencies not to disclose to the public information that is protected by IP or is otherwise sensitive or proprietary to government vendors. Indeed, the compilation of training data is a confidential commercial secret with significant competitive value. We have concerns about vendors' ability to claim trade secret protection under federal or state law if disclosure is permitted, and to that end, would encourage revision of the documentation requirements in Section 5.c.iv.a.3. We recommend relying as much as possible on testing – such as the methods contained in Section 5.c.iv.c – rather than on scrutiny of training data to provide best indications of anticipated performance by the AI model. To the extent documentation of information regarding training data is required, we suggest limiting this to summary information about the data the model was trained on and/or that demonstrates how training data is appropriate to the agency's intended use. For example, documentation could show that a model was trained on industry-specific content, such as medical literature without disclosing the specifics around the articles themselves.

Lastly, we encourage OMB to provide agencies with additional flexibility to create and evolve processes around adopting AI tools. Commercially available technologies such as privacy-enhancing technologies should be considered as a means of preserving model and AI security during the training, evaluation, and verification processes as outlined in the AI Executive Order and the recent *Guidelines for Secure AI System Development* issued by the CISA and the UK's National Cyber Security Centre (UKNCSC).[13] This would build on President's directive that "Agencies shall use available policy and technical tools, including [PETs] where appropriate, to

[13] CISA, UKNCSC, et al., *Guidelines for Secure AI System Development* (Nov. 2023) (https://www.ncsc.gov.uk/files/Guidelines-for-secure-AI-system-development.pdf).

protect privacy and to combat the broader legal and societal risks — including the chilling of First Amendment rights — that result from the improper collection and use of people's data."[14]

Comments on Additional Minimum Practices for Rights-Impacting AI.

SIIA recommends requiring the additional minimum practices apply (a) only to high-risk rights-impacting systems rather than to all rights-impacting systems and (b) only where impact assessments suggest negative impacts that require further assessment and mitigation. Government resources will be strained by requiring these steps of all rights-impacting systems and the measures contained in the minimum practices provide sufficient guardrails.

In addition, we support measures to advance equity, dignity, and fairness, and to incorporate feedback from affected groups – this is essential to build trust and public confidence in the government's use of AI – we are concerned that this requirement may prove impractical in the design and development stages. This is because much of the AI tools will be developed by non-governmental entities and the federal procurement process and budgeting deadlines present challenges. We recommend revising this language, consistent with Section 7.2 of the AI Executive Order, to avoid creating new barriers to adoption.

7. What types of materials or resources would be most valuable to help agencies, as appropriate, incorporate the requirements and recommendations of this memorandum into relevant contracts?

SIIA appreciates the thoughtful approach to federal procurement taken in the Draft AI Memo. We provide two comments on the proposed text.

First, SIIA recommends that OMB remove the reference to "copyright" in "Aligning to National Values and Law" and replace it with the umbrella term "intellectual property."[15] The use of commercial AI by the government will raise issues around trade secret and patent law. In addition, the question of copyright and AI is exceedingly complex and raises a multitude of questions that are now being considered by all three branches of the federal government. Developing a position in all of these areas will require additional time to get right.

Second, we caution OMB to amend its requirement for generative AI models to have labeling and provenance capabilities to create flexibility as the technology develops.[16] These technologies remain in their infancy and we recommend that the government avoid aligning to

[14] White House AI Exec. Order Section 2(f).

[15] Office of Management and Budget, Draft AI Mem. Section 5.d.i.

[16] Office of Management and Budget, Draft AI Mem. Section 5.d.v.B.

a single standard for achieving the goals of authentication and provenance as the technology continues to develop and different approaches may prove more effective for different use cases.

Third, OMB should ensure agencies are able to protect the data of companies and their intellectual property insofar as it has to be exposed, collected, or provided to the government.[17] This includes using contractual clauses based in the FAR and DFARS along with any agency-specific deviations or internal policy to provide an assurance of confidentiality and exemption from FOIA disclosure with all requisite authorities to hold those who intentionally, accidentally, or otherwise disclose such information accountable.

* * *

The AI Executive Order marks perhaps the most significant measure to date reflecting the United States' approach to AI governance, and we appreciate the opportunity to comment on OMB's efforts to implement responsible AI across the federal government. We look forward to continuing to work with OMB and the Administration as this effort continues. Please direct inquiries to Paul Lekas, SIIA's Senior Vice President and Head of Global Public Policy & Government Affairs, at plekas@siia.net.

[17] Office of Management and Budget, Draft AI Mem. Section 5.d.iv.