7 July 2023

To: **White House Office of Science and Technology Policy**

From: **Ed Palacio, President, IEEE-USA**

In re: ***Request for Information; National Priorities for Artificial Intelligence, Document 88 FR 34194***

IEEE-USA is pleased to submit this document in response to the OSTP's request for information (RFI), published at *88 FR 34194* (26 May 2023) soliciting input from stakeholders to help inform the federal government's update of the U.S. national priorities and future actions on AI.

IEEE-USA has responded to several federal agency requests for information and comment regarding AI systems and their deployment in our society. Those documents are referenced in our response to this RFI. Our input is focused on a select number of questions. The questions retain their original numbers as presented in the OSTP's RFI document.

IEEE-USA represents approximately 180,000 engineers, scientists, and allied professionals living and working in the US. Our members work in AI-related industries, developing and working with the emerging technologies used in artificial intelligence systems. This expertise provides us with a unique perspective on the benefits of these technologies. If you have any questions and wish to discuss our input, please contact Erica Wissolik at (202) 530-8347 or e.wissolik@ieee.org.

1. What specific measures—...?

The societal benefits of AI systems are unfairly distributed, exacerbating existing inequalities. For example, corporations with greater access to resources and data have an advantage over new competitors in all sectors. Public policies must promote equal access to data and technology. Specifically, they should address bias and discrimination in AI systems, and their benefits must be distributed fairly to create a competitive marketplace and prevent the concentration of power in the hands of a few (*see additional reference*[1]*).* Overall, IEEE believes that policies for this technology should:

1. Enable individuals and businesses to control their data, facilitate data access and portability. This allows increased competition by enabling startups and new entrants to access relevant data and compete with established players.
2. Foster an environment that supports startups and small businesses by providing access to funding, resources, and mentorship programs.
3. Enforce and strengthen antitrust laws to prevent anti-competitive behavior. This includes scrutinizing mergers and acquisitions that may lead to monopolistic practices.
4. Ensure that policies strike a balance between encouraging innovation and protection of IP.[2]
5. Implement procurement policies that consider competition and promote the participation of a diverse range of vendors; prevent vendor lock-in, encourage supplier competition.
6. Increase investments in AI research and development to support the emergence of new players in the AI market.[3]
7. Require clear disclosure of AI system capabilities, limitations, and potential biases, allowing consumers to make informed choices.

3. Are there forms of voluntary or mandatory oversight …?

(See additional reference.[4]*)*

Voluntary Self-Regulation: Includes the establishment of ethical guidelines, codes of conduct, and industry best practices. Self-regulation can be supported by independent audits, certifications, and transparency reports. Policies that should be considered that are related to self-regulation are:

1. Mandatory Disclosure and Transparency: Require AI developers and deployers to disclose relevant information about their systems to enable external scrutiny, e.g., disclosure of AI algorithms, training data sources, conflicts of interest, and potential biases.
2. Registration and Licensing: Introducing registration and licensing requirements for certain high-risk AI systems can ensure that they meet specific standards before deployment.

[1] IEEE-USA Response to National Telecommunications and Information Administration's (NTIA) request for input on how to develop a productive AI accountability ecosystem, June 2023.

[2] IEEE-USA Response to USPTO Request for Comments Regarding Artificial Intelligence and Inventorship, May 2023; and IEEE-USA Response to USPTO Request for Comments on Patenting Artificial Intelligence Inventions, October 2019.

[3] IEEE-USA's comments on the findings and recommendations of the interim report by the National AI Research Resource Task Force (87 FR 31914), https://ieeeusa.org/assets/public-policy/policy-log/2022/063022.pdf, 30 June 2022.

[4] IEEE-USA letter responding to the National Telecommunications and Information Administration's (NTIA) request for input on how to develop a productive AI accountability ecosystem, June 2023.

3. Government Incentives for Responsible AI: Including tax breaks and grants to encourage organizations to adopt responsible AI practices.
4. Independent Audits and Certification: Third-party audits and certification processes can assess AI systems for compliance with ethical and safety standards.[5]
5. Sector-specific Regulatory Frameworks: Different sectors require tailored oversight mechanisms based on their unique risks. Learning from existing regulatory frameworks in sectors like healthcare, aviation, or finance can provide valuable insight into development of effective oversight models.

6. How can AI rapidly identify cyber vulnerabilities …?

The effectiveness of AI systems depends on the availability of high-quality data, robust models, and collaboration between experts, cybersecurity professionals, and infrastructure operators. AI models trained on large-scale datasets containing information about known vulnerabilities, attack patterns, and system weaknesses, can analyze configurations, network traffic, and system logs of critical infrastructure systems to detect potential vulnerabilities. By leveraging machine learning techniques, AI can identify patterns and anomalies that indicate the presence of vulnerabilities, enabling rapid detection. AI systems that integrate with external threat intelligence feeds, security databases, and vulnerability repositories to continuously update the latest vulnerabilities can identify potential risks and prioritize remediation efforts. By analyzing the real-time data generated by critical infrastructure systems, such as network traffic, user behavior, and system logs, we can detect anomalous activities that might indicate a cyberattack or vulnerability exploitation. AI models can:

1. Leverage historical data from critical infrastructure systems to develop predictive models that estimate the likelihood of future vulnerabilities or cyberattacks. By analyzing patterns and trends, AI can identify system weaknesses that might be exploited in the future, allowing proactive mitigation and vulnerability patching before any actual attacks occur.
2. Assist in automating the process of patching vulnerabilities and applying security updates to critical infrastructure systems. By analyzing the identified vulnerabilities and understanding their potential impact, AI can generate recommendations for remediation actions and prioritize the patching process based on the level of risk and criticality.
3. Enable critical infrastructure systems to dynamically adapt their security measures based on the evolving threat landscape. By continuously analyzing real-time data, AI models can adjust security configurations, access controls, and system defenses to mitigate emerging vulnerabilities and counter new attack techniques.

9. What are the opportunities for AI to enhance equity …?

It is crucial to prioritize diversity and inclusion in AI research, development, decision-making processes, and impact assessments to identify and address potential biases. *(See additional resources.[6])*

[5] Trustworthy Evidence For Trustworthy Technology: An Overview of Evidence for Assessing the Trustworthiness of Autonomous and Intelligent Systems, IEEE, September 2022; and IEEE CertifAIEd™ a certification program for assessing ethics of Autonomous Intelligent Systems (AIS).

[6] IEEE-USA Position Statement, *Privacy, Equity, and Justice in Artificial Intelligence*, and *Artificial Intelligence: Jobs, Education, Workforce, and Diversity*, November 2021.

12. What additional considerations or measures are needed to assure that AI mitigates…?

Necessary additional considerations and measures include: *(See additional resources.[7])*

1. Techniques such as data anonymization, data augmentation, and algorithmic auditing can help identify and mitigate biases in the training data.
2. Implementing fairness metrics, conducting bias assessments, and providing explanations for AI-generated decisions can enhance transparency and accountability.
3. Developing and adhering to ethical guidelines and codes of conduct specific to usage in various domains.
4. Regular monitoring and evaluation of AI systems in specific domains are essential.
5. Public consultation and diverse representation on AI governance bodies is crucial.
6. Promoting AI literacy and awareness fosters understanding of the potential risks and challenges associated with AI systems.

15. What are the key challenges posed to democracy by AI systems?...

1. AI-generated content, such as deepfakes and misinformation campaigns spread disinformation and manipulate public opinion, undermining the integrity of the information ecosystem.
2. AI systems can perpetuate existing biases and discrimination, leading to unequal treatment and access to opportunities for certain groups.
3. Improper handling and use of vast amounts of data raises concerns about privacy.
4. The deployment of AI systems can consolidate power in the hands of a few dominant entities, limiting competition and potentially creating asymmetries that impact democratic processes and economic fairness.

To address these challenges, the US government should: *(See additional resources.[8])*

1. Implement robust regulations that promote transparency, accountability, and fairness.
2. Use standards[9] and guidelines for responsible AI development and deployment to prevent the spread of disinformation, ensure algorithmic fairness, and protect privacy rights.
3. Invest in public awareness campaigns and educational programs that promote critical thinking, media literacy, and digital skills.
4. Bolster cybersecurity measures to protect critical infrastructure, electoral systems, and information platforms from AI-driven attacks and manipulation. Collaborate with technology companies to develop robust security protocols and detection mechanisms.

[7] IEEE-USA letter responding to the National Telecommunications and Information Administration's (NTIA) request for input on how to develop a productive AI accountability ecosystem, June 2023; IEEE-USA Position Statement: Privacy, Equity and Justice in Artificial Intelligence; and *Trustworthy Evidence For Trustworthy Technology: An Overview of Evidence for Assessing the Trustworthiness of Autonomous and Intelligent Systems,* IEEE, September 2022.

[8] IEEE-USA letter responding to the National Telecommunications and Information Administration's (NTIA) request for input on how to develop a productive AI accountability ecosystem, June 2023; IEEE-USA Position Statement: Privacy, Equity and Justice in Artificial Intelligence; and *Trustworthy Evidence For Trustworthy Technology: An Overview of Evidence for Assessing the Trustworthiness of Autonomous and Intelligent Systems,* IEEE, September 2022.

[9] IEEE Standards Association portfolio of AIS technology and impact standards and standards projects.

5. Promote the development and adoption of ethical AI practices that prioritize fairness, transparency, and accountability. Encourage interdisciplinary collaboration among researchers, policymakers, and industry stakeholders to address bias, discrimination, and ethical concerns associated with AI systems.
6. Establish collaborative platforms for dialogue, knowledge sharing, and public policy development to ensure diverse perspectives and expertise are considered.
7. Foster participatory governance models that involve public consultation, deliberation, and citizen input to ensure that AI systems align with democratic values and serve the public interest.

16. What steps can the United States take to ensure that all individuals …?

(See additional resources.[10])

Promoting economic growth and good jobs:

1. Promote Digital Literacy: Provide accessible resources and training to enhance understanding of AI technologies.
2. Expand STEM Education: Integrate AI-related topics into school curricula; promote hands-on learning experiences, coding skills, and problem-solving abilities.
3. Foster Lifelong Learning: Support AI-related online courses, vocational training programs, and educational platforms.
4. Bridge the Digital Divide: Expand broadband infrastructure and ensure affordable internet access for underserved communities.
5. Public-Private Partnerships: Foster collaborations between government, educational institutions, and industry to develop AI systems training programs, internships, and apprenticeships.

17. What will be the principal benefits of AI …?

Benefits include increased efficiency and productivity; improved healthcare; enhanced education; advanced sustainable transportation networks; broader availability of goods and services. and reduced costs. For example, pattern-matching and predictive AI has shown promise in modeling protein folding and other clues to drug-discovery. To capture the benefits, the United States should consider:

1. Increase funding for AI R&D, government grants, partnerships with academic institutions and industry - particularly the less well-endowed or necessarily less profitable – and support for startups.
2. Foster public and private partnerships to share expertise, resources, and best practices.
3. Establish a regulatory framework that addresses privacy, security, competition, fairness, transparency, and accountability to protect consumer rights and mitigate potential risks.
4. Invest in education and workforce training programs to develop a skilled workforce.
5. Encourage and publicly educate about the benefits and pitfalls of open data initiatives while protecting privacy and security.

[10] IEEE-USA letter responding to the National Telecommunications and Information Administration's (NTIA) request for input on how to develop a productive AI accountability ecosystem, June 2023; and IEEE-USA Position statement, Artificial Intelligence: Jobs, Education, Workforce, and Diversity.

6. Provide resources and incentives to support public services, small businesses and startups in adopting AI technologies.

18. How can the United States harness AI …?

1. Invest in reskilling and upskilling programs to ensure that workers have the necessary skills, including providing training in areas such as data literacy, digital skills, and AI-specific knowledge. Collaboration between government, educational institutions, and industry can help design effective training programs.
2. Assist workers in transitioning to new roles or industries by providing job placement services, career counseling, and financial support for retraining. Programs like income support, job matching, and unemployment benefits can help alleviate the short-term challenges faced by workers during transitions.
3. Emphasize the augmentation of human capabilities rather than outright replacement. Promote the idea of human-machine collaboration. This approach ensures that workers remain essential and valued contributors in the workplace.
4. Encourage businesses to adopt ethical and responsible practices that prioritize fairness, transparency, and accountability. Implement guidelines and regulations that prevent discriminatory practices, protect worker rights, and ensure the responsible use of AI in employment decisions.
5. Promote the development of AI systems that are inclusive and accessible to all workers, including those with disabilities or specific needs.
6. Establish robust data governance frameworks to protect worker privacy and prevent unauthorized use of personal data.
7. Foster ongoing dialogue and collaboration among policymakers, industry leaders, labor unions, worker representatives, and other stakeholders.

19. What specific measures—such as sector-specific policies, standards, and regulations—are needed …?

1. Develop sector-specific policies that foster innovation and AI adoption in key areas such as healthcare, transportation, education, finance, and energy – particularly in underfunded public services. These policies should encourage research and development, provide regulatory clarity, and support the deployment of AI technologies in a manner that benefits both businesses and consumers.
2. Establish industry standards and guidelines to ensure the ethical and responsible development and use of AI systems. These standards can cover areas such as transparency, fairness, privacy, security, and accountability. Standards organizations, government agencies, and industry associations can collaborate to develop and promote these standards.
3. Create a regulatory framework that strikes a balance between fostering innovation and protecting other public interests, including competition. This includes addressing issues related to data privacy, security, algorithmic transparency, and potential biases and concentration in AI systems. Regulatory bodies such as the Federal Trade Commission (FTC), the Federal Communications Commission (FCC), and the Consumer Financial Protection Bureau (CFPB) can play a role in developing and enforcing these regulations.
4. Increase investments in AI research and development to fuel innovation and advance the state of the art. This can be done through government funding programs, grants, and partnerships with academic and industry research institutions. The National Science Foundation (NSF), the National Institutes of Health (NIH), and the Department of Defense (DoD) are examples of entities that can support such initiatives.
5. Enhance education and workforce development programs to equip individuals with the skills needed to thrive in an AI-driven economy. This includes promoting STEM education, expanding AI-related curricula, and

supporting vocational training programs. Collaboration between government, educational institutions, and industry is crucial to ensure alignment with industry needs.

6. Foster a competitive environment that encourages entrepreneurship and the growth of AI startups within ethical bounds. This can involve measures such as creating incentives for startups, reducing regulatory barriers, and promoting access to funding and resources for small and medium-sized enterprises (SMEs). It also may include consideration of sharing of large data bases collected by large platforms from the public through their access at different points in public networks.
7. Facilitate public-private partnerships to drive AI innovation and adoption. Collaborative initiatives between government agencies and private companies can accelerate the development and deployment of AI technologies, as well as address societal challenges and ensure public benefit.
8. Improve broadband connectivity and digital infrastructure across the country to ensure equitable access to AI technologies and benefits. This includes investing in the expansion of high-speed internet access, especially in underserved areas.

20. What are potential harms and tradeoffs …?

While AI offers significant benefits, potential harms and tradeoffs are:

1. AI automation may lead to job displacement as certain tasks and roles become automated. This can impact various industries and job sectors, potentially leading to unemployment or the need for workers to transition into different roles.
2. The deployment of AI technologies may require workers to acquire new skills and adapt to changing job requirements. This poses challenges for individuals who lack the necessary skills or face barriers to accessing training and education programs.
3. AI systems can inherit biases present in training data, resulting in discriminatory outcomes in areas such as hiring, lending, and law enforcement. This perpetuates inequality and discrimination if not properly addressed and mitigated.
4. The widespread use of AI involves processing and analyzing vast amounts of personal data, raising concerns about privacy and data security.
5. AI technologies are often developed and controlled by a few dominant players, leading to a concentration of power. This can have implications for competition, market dynamics, and influence over societal decision-making.

To address these issues, consider the following: *(See additional resources.[11])*

1. Implement robust training and education programs to help workers acquire the skills needed for the jobs of the future. Encourage partnerships between educational institutions, industry, and government to provide accessible and relevant training opportunities.
2. Establish job transition programs to support workers who are displaced by AI-driven automation.

[11] IEEE-USA Position Statement, *Privacy, Equity, and Justice in Artificial Intelligence*, and *Artificial Intelligence: Jobs, Education, Workforce, and Diversity*, November 2021.

3. Enhance social safety nets to provide a cushion for workers facing job displacement or economic instability. This may involve expanding unemployment benefits, healthcare coverage, and other forms of social assistance.
4. Promote entrepreneurship and innovation to create new job opportunities and encourage the growth of AI-related startups. This can be supported through funding programs, access to resources, and streamlined regulatory processes for startups.
5. Encourage organizations to adopt ethical and responsible AI guidelines to mitigate bias, ensure transparency, and promote fairness. Establish regulations that hold AI systems accountable for their impacts on workers and society.
6. Foster open and inclusive dialogue involving government, industry, labor unions, academia, and civil society to address the challenges and tradeoffs associated with AI deployment.

22. What new job opportunities will AI create? …

While AI technologies may automate certain tasks and job functions, they potentially augment and enhance human capabilities, leading to the emergence of new professions, e.g. AI trainers and supervisors who curate and annotate data, ensure quality control, and provide oversight; AI ethicists and policy experts who ensure accountability, and address potential biases and societal impacts; and AI support and maintenance experts who provide technical support, system monitoring, and AI system maintenance.

To strengthen the AI workforce and ensure equal opportunities for all Americans, invest in AI education and training programs at all levels, from primary education to higher education and vocational training; broaden access to scholarships, mentor programs and initiatives that promote diversity; support collaboration between educational institutions and industry to align AI education with industry needs; enable lifelong learning and reskilling for current workers; and foster entrepreneurship and job creation through investments in AI research and development.

23. How can the United States ensure adequate competition…?

Innovating in public services: *(See additional resource.[12])*

24. How can the Federal Government effectively and responsibly leverage …?

Conduct a comprehensive assessment of existing federal services and missions to identify areas where AI systems can be applied effectively.

1. Promote collaboration and information sharing among federal agencies to pool resources, knowledge, and expertise in AI. Establish interagency working groups or task forces to coordinate AI initiatives, share best practices, and avoid duplication of efforts.
2. Invest in the federal workforce through AI training programs, partnerships with academic institutions, and recruitment of AI professionals..
3. Establish AI Centers of Excellence within federal agencies to drive adoption, innovation, and best practices.

[12] IEEE-USA letter responding to the National Telecommunications and Information Administration's (NTIA) request for input on how to develop a productive AI accountability ecosystem.

4. Streamline data sharing practices among federal agencies, while ensuring strong data governance and privacy protections.
5. Launch pilot projects in key areas to test the feasibility and effectiveness of AI applications.
6. Improve workforce efficiency by identifying routine and repetitive tasks that can be automated using AI technologies.
7. Develop new and use existing guidelines and standards for the ethical use of AI within the federal government.
8. Foster partnerships with private sector companies, research institutions, and academic organizations to leverage expertise, share knowledge, and access cutting-edge technologies and research.

25. How can Federal agencies use shared pools …?

1. Establish communities of practice bringing together experts, practitioners, and stakeholders from different agencies to facilitate knowledge sharing.
2. Encourage the sharing of anonymized and aggregated data sets among agencies to facilitate development and training of AI models while adhering to security protocols.
3. Foster collaborative research and development efforts to address common challenges.
4. Establish Centers of Excellence (CoEs) dedicated to AI to serve as hubs of expertise, providing guidance, technical support, and training to other agencies on implementation.
5. Develop standardized data governance frameworks and protocols that facilitate data sharing and interoperability among agencies. Establish common data standards, metadata frameworks, and data catalogs to streamline data access and utilization.
6. Develop training programs and workshops to enable cross-pollination of skills and knowledge. These programs can provide opportunities for upskilling and reskilling in AI technologies and practices.
7. Explore the creation of shared AI infrastructure that can be used by multiple agencies, including shared computational resources, cloud-based AI platforms, and tools for data processing and model development.
8. Collaborate on the development of ethical guidelines for deployment.

26. How can the Federal Government work with the private sector…?

Responsible procurement should be a collective action standard that requires purposeful and proactive due diligence (layered on top of adapted existing acquisition processes). Federal Acquisition Regulation (FAR) has not updated or adapted PART 39 Acquisition of Information Technology components to the special requirements, opportunities and challenges of AI and ADS. AI and ADS present new challenges for public agencies procuring advanced "information technology" and procurement of AI and ADS solutions making critical decisions.[13]

[13] Critical decisions are those that have legal, material, or similarly significant effects on individual and group lives concerning access to, or the cost, terms, or availability of products and or services. High stakes contexts using AI tools that apply critical decisions can have high risk impacts on vulnerable populations. Critical decision domains include, but are not limited to education, employment, healthcare, family planning, financial services, housing, government services, public services, critical infrastructure, essential utilities, law enforcement, justice, immigration, legal services, biometric identification, and public safety components.

Using the IEEE-SA P3119 Standard for the Procurement of AI and ADS as reference, we recommend adapting FAR processes as such:[14]

Pre-Procurement

Collaboratively Update Part 39 of the FAR by engaging AI procurement experts, the public, and a multi-stakeholder procurement team (internal and external experts) to review the challenges and opportunities that AI and ADS bring to public procurement processes.

Conduct a Pre-procurement collaboration and Problem Definition Process IEEE SA P3119 Standard in development can be used *in a sandbox environment with the Federal Government* to test FAR adaptations to the procurement of AI/ADS.

Procurement

Critically Evaluate vendors' corporate AI governance maturity and the risks posed by vendors with undeveloped competence or unwillingness to provide attestations of their AI governance maturity.

Critically Evaluate procurement contract language. Risks identified in prior pre-procurement and procurement processes should be mitigated through specific, measurable, attainable, reasonable, and time-bound contractual language. Past RFP contract language that reflects the acquisition of traditional information technology does not currently protect the public interest. When procuring AI that serves the public sector, the contract language[15] must be adapted to purposefully protect the public interests. Contracts should also contain requirements for ongoing monitoring during the life of the contract as well as provisions for timely redress of adverse incidents and pre-approval of any system version updates.

Post Procurement

Proactively Monitor the intended and potential unintended, misuse, disuse, and abuse of the AI solution during the life of the contract. In coordination with vendors AND third-party auditors, the Federal government should proactively monitor the data, model, and application of the AI and/or ADS solution and system. Independent third-party auditing (conducted annually under confidentiality agreements) can be used to verify compliance and validity of system performance.

29. Do you have any other comments …?

Several key commercial and technological developments are transforming various industries, and new applications have the potential to create significant opportunities for users. The emergence of large language models (LLMs) like ChatGPT have "democratized" the use of generative AI, making large, inexpensive models available to millions of users. This development enables "weaponization" of AI through "deepfakes." Of danger is the lack of understanding among users that the results of their prompts are not founded on reason or facts. This provides competitive power to the owners of the foundational models with access to enormous data sets and computing resources. Not only do these owners control access to the models and affect the user business models (e.g., "fine tuning," use of cloud services), but they may propose regulations that are acceptable to them but less favorable to new entrants or users ("regulatory capture").

[14] The IEEE P3119 Standard offers additional details, https://standards.ieee.org/ieee/3119/10729/.

[15] AI Procurement: Essential Considerations in Contracting, Center for Inclusive Change.

Individuals facilitating their services using generative tools often do so without basic understanding of their limitations; even technology savvy operators may deploy AI products and services without adequate knowledge or resources to do so responsibly or accountably. Additionally, these operators may and likely do fall well below the threshold for regulatory review and enforcement or, where rights of private action even exist. Further, reports are already surfacing that fraudulent or criminal operators are using these highly accessible AI tools to perpetuate scams and other violative or criminal schemes, including the sale of hacked ChatGPT credentials on the dark web. The lack of meaningful regulation and enforcement combined with the easy availability of tools enable AI to be weaponized.

Therefore, meaningful governance of LLMs, chatbots, and AI acceleration and deployment tools is critically important. Significant government monitoring and enforcement, including under existing consumer protection, competition, privacy, and other laws, is urgently needed. Consideration may be given to the large platforms sharing with new or specialized operators the data (in appropriate form and under appropriate terms) that they have collected through their access on the public networks, which the current direction of data subject rights regulates. Given the limited resources (and challenge to jurisdiction) of existing regulatory agencies, suitably limited private rights of action such as effectively applied under the Clayton Act may provide needed, adaptive guardrails against irresponsible, unaccountable, fraudulent, and criminal AI practices and uses.