TECHNET
THE VOICE OF THE
INNOVATION ECONOMY

1420 New York Avenue NW, Suite 825
Washington, D.C. 20005
www.technet.org | @TechNetUpdate

February 2, 2024

Information Technology Laboratory
ATTN: AI E.O. RFI Comments
National Institute of Standards and Technology
100 Bureau Drive, Mail Stop 8900
Gaithersburg, MD 20899

RE: NIST AI Executive Order

To Whom It May Concern:

TechNet appreciates the opportunity to comment on the National Institute of Standards and Technology's (NIST) request for information on NIST's assignments under sections 4.1, 4.5, and 11 of the Executive Order Concerning Artificial Intelligence. Many of TechNet's members are our nation's leading AI developers, deployers, researchers, and users.

TechNet is the national, bipartisan network of technology CEOs and senior executives that promotes the growth of the innovation economy by advocating a targeted policy agenda at the federal and 50-state level. TechNet's diverse membership includes dynamic American businesses ranging from startups to the most iconic companies on the planet and represents over 4.2 million employees and countless customers in the fields of information technology, artificial intelligence, e-commerce, the sharing and gig economies, advanced energy, transportation, cybersecurity, venture capital, and finance.

Millions of Americans have been using AI for years to navigate traffic, search the internet, undertake research, conduct a spell check, vacuum their home, and discover new music. AI is also being used to predict severe weather more accurately, protect critical infrastructure, defend against cyber threats, and accelerate the development of new medical treatments, including life-saving vaccines and ways to detect earlier signs of cancer.

NIST is delegated several important responsibilities in President Biden's recent Executive Order on "Safe, Secure, and Trustworthy Artificial Intelligence." This EO will bolster our workforce through investments in upskilling and training programs and our ability to attract and retain the world's best talent, policies TechNet has long championed. It will also lower the barrier to entry for AI research through the pilot National AI Research Resource (NAIRR), strengthen our nation's cyber defenses, especially in the financial sector, and improve health care and education

outcomes. We believe America must be the global leader in setting standards for the responsible development and deployment of AI. TechNet looks forward to working with the Biden Administration and Congress to ensure AI continues to deliver benefits for all Americans.

Existing Legal Protections

There has been a rapid rise in public interest in AI due to advancements in generative AI technologies. We appreciate NIST's work to update their existing standards for generative AI. We want to stress that the use of AI in furtherance of unlawful behavior is already prohibited and actionable under existing laws, even in the absence of AI-specific regulation. For example, many existing anti-discrimination laws apply to AI models in important areas, including education, healthcare, employment, housing, financial services, policing and criminal justice, and access to goods and services.[1] Agencies should utilize existing legal requirements when considering AI management practices and seek to build upon legal precedent for addressing this emerging technology.

Several federal leaders have stated their intent to use existing laws to regulate AI; for example, on April 25, the Consumer Financial Protection Bureau, the Department of Justice's Civil Rights Division, the Equal Employment Opportunity Commission, and the Federal Trade Commission issued a joint statement outlining how their existing enforcement authorities apply to automated systems.[2] In addition, National Labor Relations Board (NLRB) General Counsel Jennifer Abruzzo has stated that she will "… apply the [National Labor Relations] Act to protect employees from intrusive electronic monitoring and automated management practices…".[3] Additional oversight in these areas should not be duplicative or create inconsistent or conflicting requirements.

The private sector must comply with existing legal requirements, including laws protecting privacy and preventing discrimination. Accordingly, TechNet members are designing, developing, deploying, and using AI technology cautiously and only after rigorously assessing the benefits and risks of implementation. The use of AI applications falls within the scope of these legal protections, and we urge NIST to ensure that any new guidance it produces will be within these prevailing frameworks and should not seek to extend existing law.

---

[1] Several existing enforcement statues were outlined in the National AI Advisory Committee's Year One Report: *Civil Rights Act of 1964, Equal Educational Opportunities Act, Americans with Disabilities Act, Individuals with Disabilities in Education Act, Genetic Information Nondiscrimination Act, Immigration and Nationality Act's Anti-Discrimination Provision, Fair Housing Act, Equal Credit Opportunity Act, Violent Crime Control and Law Enforcement Act,* and the *Omnibus Crime Control and Safe Streets Act.*

[2] Chopra, Rohit, Kristen Clarke, Charlotte Burrows, and Lina Khan. "JOINT STATEMENT ON ENFORCEMENT EFFORTS AGAINST DISCRIMINATION AND BIAS IN AUTOMATED SYSTEMS." FTC.Gov. April 25, 2023. https://www.ftc.gov/legal-library/browse/cases-proceedings/public-statements/joint-statement-enforcement-efforts-against-discrimination-bias-automated-systems.

[3] Office of Public Affairs. "NLRB General Counsel Issues Memo on Unlawful Electronic Surveillance and Automated Management Practices." National Labor Relations Board. October 31, 2022. https://www.nlrb.gov/news-outreach/news-story/nlrb-general-counsel-issues-memo-on-unlawful-electronic-surveillance-and.

Building upon the NIST AI RMF

Many AI stakeholders apply the NIST Artificial Intelligence Risk Management Framework (NIST AI RMF) to review and examine their systems for determining and addressing risk throughout a system's lifecycle. The NIST AI RMF supports AI developers, deployers, and other stakeholders in this effort by providing a risk-based, voluntary approach to incorporate trustworthiness and accountability benchmarks into the entire lifecycle of an AI system. In addition, the NIST AI RMF appropriately recognizes that the level of risk among different AI use cases can vary significantly.

Similar to the process it used when developing its Cybersecurity and Privacy Engineering Frameworks, NIST developed its AI RMF in collaboration with key AI researchers, developers, and the broader technology industry. The public-private partnership fostered by NIST and the transparent development process ultimately led to a strong and forward-looking document. We advise that as NIST looks to develop a companion resource to the AI RMF on generative AI, utilizing a similar process as a model for policy development. We further urge NIST to consider and build in pathways for evolving the resulting framework to an international technical standard. NIST can achieve this by engaging experts already involved in the development of international technical standards.

We also urge that any updates to the NIST AI RMF provide specific definitions of the practices they advise, such as red-teaming, field testing, provenance tracking, etc. and that these definitions are drawn upon or at least consistent with those being identified in international technical standards or those currently in development in bodies such as ISO-IEC/JTC1/SC42. While many in the industry are already familiar with these concepts and their applications, there can be differences in understanding between different organizations. It is also important to have clear definitions in order for this document to be adoptable by a wide audience and around the world.

Further, TechNet appreciates NIST's launch of the Trustworthy and Responsible AI Resource Center to support AI developers and users in implementing the AI RMF and the development of trustworthy and responsible AI technologies.

Unique Roles in the AI Ecosystem

We appreciate NIST's attention to the unique roles amongst AI actors and the need for guidance for their specific positions in the AI system lifecycle. We believe it is crucial to differentiate responsibilities between developers, deployers, and users. Careful consideration must be given to delegating regulatory responsibility that aligns with the roles and interactions of these entities. In order to implement effective safety policies, it is important for all of these actors to work together and have clear roles to maintain responsible AI systems. It is also important to note that the AI startup ecosystem is vital to maintaining America's competitive edge in

the economy. We would appreciate NIST's consideration of the potential implications of policies for small and mid-size businesses.

AI Ready Data

TechNet supports the government development of "AI Ready Data." The federal government is one of the biggest producers of data in the world, and these important datasets are already fueling innovation in the public and private sectors. As we move to greater deployment of AI systems, ensuring this data is well-organized will allow these modern tools to deliver faster, cost-effective, and more accurate insights. This is notably important for the development of trustworthy generative AI systems. For example, it is estimated that some commercial generative AI systems have been trained on about 45 terabytes of text data.[4] We encourage NIST and other agencies to implement AI-ready data strategies to ensure that they can properly utilize systems, as well as build upon the efforts manifest in Data.gov and make further datasets public when appropriate to increase AI research and development and support the deployment of trustworthy AI.

Independent Assessments

We appreciate NIST's efforts to develop guidance and benchmarks for evaluating AI capabilities and believe this effort can build upon existing industry processes. However, TechNet members believe that it is premature to mandate independent third-party auditing of artificial intelligence systems. Mandating an independent audit before appropriate technical standards and conformity assessment requirements are established could open AI systems to trade secrets theft and inaccurate audit reports. We look forward to partnering with NIST and other evaluation organizations to develop additional research on the best way to assess AI systems.

Scoping

We also want to highlight the importance of clearly defining artificial intelligence. Two key documents that policymakers repeatedly point to, the White House's Blueprint for an AI Bill of Rights and NIST's AI Risk Management Framework, utilize different definitions of AI. While both documents offer voluntary, non-binding guidance, these differing definitions — both issued by the same administration — can send confusing messages to AI developers and deployers. Compounding this confusion is that aspects of the AI Bill of Rights have been raised by the Biden Administration in the G7 Principles, creating international misdirection.

[4] Cooper, Kindra. 2021. "OpenAI GPT-3: Everything You Need to Know." Springboard Blog. November 1, 2021. https://www.springboard.com/blog/data-science/machine-learning-gpt-3-open-ai/.

We advise NIST to utilize the latest definition developed by the Organisation for Economic Co-operation and Development (OECD) in November 2023. This definition states that "An AI system is a machine-based system that for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations or decisions that can influence physical or virtual environments. Different AI systems vary in their levels of autonomy and adaptiveness after deployment." OECD's prior definition from 2019 was utilized for the development of the NIST AI RMF definition of AI, alongside ISO/IEC 22989. [5] We advise the use of the OECD definition because it was developed through close coordination with the experts from the AI community, and it would allow for domestic and international consistency. Adopting the OECD definition across government will help provide greater clarity for the public's understanding of AI systems.

Conclusion

We look forward to working with you on AI policy and appreciate the opportunity to discuss this innovative technology. We stand ready to serve as a resource to you in your examination of this important issue. Thank you for your consideration of our perspective.

Sincerely,

Carl Holshouser

Executive Vice President and Corporate Secretary

[5] The AI RMF defines an AI system as an engineered or machine-based system that can, for a given set of objectives, generate outputs such as predictions, recommendations, or decisions influencing real or virtual environments. AI systems are designed to operate with varying levels of autonomy.