July 19, 2019

Elham Tabassi
Acting Chief of Staff, Information Technology Laboratory
National Institute of Standards and Technology
100 Bureau Drive
Gaithersburg, MD 20899

RE: A Plan for Federal Engagement in AI Standards - Draft for Public Review

Dear Ms. Tabassi,

The Center for Security and Emerging Technology appreciates the opportunity to comment on NIST's draft Plan for Federal Engagement in AI Standards. The draft Plan is a welcome step toward greater federal involvement in the development of AI standards. As it points out, American leadership in AI requires active federal engagement in the standards process. CSET supports NIST's call for robust federal investment in AI trustworthiness research, and we agree that NIST and other federal agencies should prioritize standard-setting processes that are open, inclusive and multi-channel.

As the federal government's principal agency for standardization and a historic leader in AI and computing research, NIST is well positioned to spearhead federal engagement in AI standards development. To help ensure success, we offer the following suggestions for the final Plan:

1. **Expand the draft Plan's discussion of foundational research, and encourage peer federal agencies to support this research.** Standard setting requires clear technical and conceptual foundations. In the case of AI, these foundations are far from complete, especially with regard to AI safety and trustworthiness. More research needs to be done before effective standards can be developed in these areas. Accordingly, we encourage NIST to emphasize further and expand on the draft Plan's discussion of foundational research. In particular, NIST should consider explaining in greater detail how it plans to fund and coordinate foundational research on trustworthiness and related tools and infrastructure. In addition, NIST should consider explicitly calling on peer federal agencies to fund foundational research in subsections 2(B) (Prioritizing Levels of U.S. Government Engagement in AI Standards) and 2(C) (Practical Steps for Agency Engagement in AI Standards).

2. **Propose a National AI Testbed.** As the draft Plan observes, AI testbeds have a vital role to play in standard setting. We urge NIST to propose a National AI Testbed in the final Plan. Given its experience in maintaining collaborative research environments, its access

to datasets and other resources unique to the federal government, and its ability to meet the distinct needs of both industry and government, NIST is well placed to establish and maintain this Testbed. The Testbed would serve as a central repository for the federal resources and tools needed for AI standards development, complementing the work of the Standards Coordinator proposed in subsection 3(1) of the draft Plan. The Testbed would also facilitate the public-private collaboration necessary for foundational research and provide a secure way for researchers to access models with dual-use risks. And, by facilitating the secure pooling of sensitive data and tools, the Testbed would enhance American researchers' access to critical resources, thereby making the U.S. AI industry more competitive.

3. **Emphasize engagement in international standard setting.** The draft Plan advises federal agencies to "strategically engage with international parties to advance AI standards for U.S. economic and national security needs." American leadership in international standard setting will both reduce global risk by creating a common understanding of what constitutes trustworthy AI *and* benefit U.S. companies and interests, whose products and access to foreign markets will be affected by international standards. Given the unique value of international engagement, the Plan should further emphasize federal involvement in international standards development processes. We also recommend that NIST propose specific venues to prioritize for engagement, or provide a timeframe or process for selecting these venues.

4. **Emphasize engagement in areas that industry is less likely to tackle on its own.** As the draft Plan notes, private industry plays a critical role in AI standard setting. However, in some areas, the private sector may underinvest. We encourage NIST to stress federal involvement in two of these areas. First, commercial pressure to bring AI products to market quickly, along with underdeveloped technical foundations, may lead industry to deprioritize investment in AI safety standards. In fact, the private sector's early steps toward AI standards, such as the MLPerf benchmarking initiative, have largely focused on issues such as interoperability and training performance rather than safety and security. Second and relatedly, the private sector may be more likely to neglect standards development in domains that require expensive and uncertain basic research. As discussed above, NIST and its peer agencies should address this potential gap by supporting foundational research for AI standards.

5. **Advocate performance-based standards when discussing timing concerns.** Section 1(C) of the draft Plan (How Are Technical Standards Developed?) notes that premature standards development may stifle innovation. Favoring performance-based standards over prescriptive standards can mitigate this risk. By building standards around desired outcomes rather than technological mandates, performance-based standards can promote

these outcomes even as AI technologies continue to evolve. We suggest discussing this dynamic and reiterating the value of performance-based standards in section 1(C).

We thank NIST for the opportunity to comment on the draft Plan. We look forward to supporting NIST and its peer agencies in the AI standard-setting process. If we can be of any further help as the final Plan is prepared, please do not hesitate to contact Zachary Arnold at zachary.arnold@georgetown.edu or 202-687-0695.

CENTER FOR SECURITY AND EMERGING TECHNOLOGY (CSET)
WALSH SCHOOL OF FOREIGN SERVICE · GEORGETOWN UNIVERSITY
STE 440 · 25 MASSACHUSETTS AVENUE NW · WASHINGTON, D.C. 20009