July 19, 2019

MITRE Corporation comments on draft federal engagement plan on AI Standards

For additional information about this response, please contact:
Duane Blackburn, S&T Policy Analyst
The MITRE Corporation
7596 Colshire Drive
McLean, VA 22102-7539

dblackburn@mitre.org
(434) 964-5023

This page is intentionally blank

MITRE Comments on Draft Plan for Federal Engagement in Developing Technical Standards and Related Tools for AI Technologies

COMMENT #	NAME OF COMMENTER	TYPE i.e., Editorial Minor Major	LINE # PAGE etc.	RATIONALE for CHANGE	PROPOSED CHANGE (specific replacement text, figure, etc. is required)
1	MITRE Corporation	Editorial	Page 4, Line 25	Typo – delete second "IS".	WHY IS A PLAN FOR FEDERAL ENGAGEMENT IN AI TECHNICAL STANDARDS NEEDED?
2	MITRE Corporation	Editorial	Page 4, Line 45-47	Sentence makes no sense as written. Delete last half of sentence.	It focuses on the Federal government's role in advancing AI standards and priorities.
3	MITRE Corporation	Minor	Page 4, Line 48.	This definition is not consistent with the definition provided in Appendix I, which is better.	…for the purposes of this plan, AI technologies and systems are considered to comprise of software and/or hardware that perform functions normally associated with human intelligence, such as reasoning, learning, and self-improvement. Such functions include problem solving, prediction, perception, planning, cognition, learning, and communication. Examples…
4	MITRE Corporation	Minor	Page 5, Line 63	A critical aspect of ensuring trustworthiness of AI-related technologies is that they be perceived as fair and unbiased.	Add "fairness" to the list of characteristics (Note: you'd also thus want to add "fairness" to P8, Footnote 10.)
5	MITRE Corporation	Minor	Page 5, Line 63	Another important aspect of trustworthiness is the overall competency of the system. An incompetent system cannot and should not be trusted.	Add "competency" to the list of characteristics (Note: you'd also thus want to add "competency" to P8, Footnote 10.)
6	MITRE Corporation	Minor	Page 5, Line 73	There are different classes of standards. Perhaps the document should mention that there are different classes of standards and list them.	Add "There are many different types of technical standards related to AI to include design and construction, test methods and techniques, usability, interoperability/interface, risk assessment, and accepted practices for engineering processes."
7	MITRE Corporation	Minor	Page 5, line 83	Section C meanders, in part by repeating material found elsewhere which is not relevant to the section title.	LL 93—97 can be deleted with no loss in meaning. LL 98-106 and 115-121 properly belong in Section B, after considerable pruning.
8	MITRE Corporation	Minor	Page 6, Line 122	The Section 1D title asks "What Standards Are Needed?", but the subsequent text provides no answers.	There needs to be at least a few explicit statements about areas that need standards in order to advance.
9	MITRE Corporation	Minor	Page 7, Line 153	No citation. (There's also an extra space between from and the)	". . . the NIST Request for Information (Appendix V), the NIST AI Standards Workshop (Appendix VI), . . . "

10	MITRE Corporation	Minor	Page 8, Line 173	Lines 160-161 in page 7 mention that *"some [areas] are more primed for standards development than others."* As a result, Table 1 does not explicitly list *security*. Instead, *security* is included as part of *trustworthiness*, which also includes aspects, such as *safety*, that are explicitly listed in Table 1. While *security* is at a formative stage (cf. lines 165-166), we also believe that AI security standards are needed (e.g., to help consumers understand the extent to which an AI-driven system has been protected from known attacks). Hence, Table 1 should list the need for security-related standards even if the corresponding foundations are not mature. The addition of *security* would likely contribute to the kind of innovation that is needed in this area. Such emphasis would be consistent with the first statement in one of the main objectives of EO 13859 (cited in lines 860-863, page 28): "***Ensure that technical standards minimize vulnerability to attacks from malicious actors*** *and reflect Federal priorities for innovation, public trust, and public confidence in systems that use AI technologies; …"*	Include a row in Table 1 for *Security* indicating that standards in this area are not available.
11	MITRE Corporation	Major	Page 8, Lines 173 and 179	As previously mentioned, Section *1.D (WHAT TECHNICAL STANDARDS ARE NEEDED?)* does not answer the question succinctly. One way to do so could be to modify Tables 1 and Table 2 to list the areas where AI standards are needed. Tables 1 and 2 should list multiple coverage levels rather than the two categories currently included (*Available; Being Developed*). The fact that standards in a category are "Available" does not clarify the extent to which more standardization efforts are needed under that category.	Modify Table 1 description as: *Needed Technical Standards Related to AI*. Similarly, Table 2's description can be modified as: *Additional AI-related Standards Needed to Inform Policy Decision*. Also, the columns should reflect multiple necessity levels. For example, the columns can be: *"No standards available"; "Inadequately covered by standards"; "Adequately covered by standards."*
12	MITRE Corporation	Major	Page 9, Line 212	There is no mention of risk assessment, assurance cases, or how to characterize the operational environment. This will be especially important when AI is used in operational technology. There is a mention of management of risk on page 11, line 273 but that under addresses the importance and complexity of the issue.	
13	MITRE Corporation	Editorial	Page 11, Line 256	Delete confusing, superfluous words.	". . . often captured as principles . . . "

14	MITRE Corporation	Minor	Page 12, line 297	The U.S. Government has a role in ensuring that safety and security risks are understood.	
15	MITRE Corporation	Major	Page 14, line 387	There is no mention of the critical role the Federal Government plays in recognizing, endorsing, and acceptance industry consensus standards. Industry motivation decreases if the government does not endorse where appropriate. Government endorsement is critical for continued industry engagement and investment in the standards development process.	Add language about the Government role in endorsing standards
16	MITRE Corporation	Major	Page 16, line 450+	For the most part these recommended actions are not very actionable or specific in terms of explicit initiatives that should be undertaken or continued. This is the meat of the document. However, most of the actions are very generic, almost philosophical. In many cases they read like guiding principles. e.g., "Make maximum use of existing standards that are broadly adopted by industry sectors that can be used or evolved within the next context of AI solutions". There are some that are very specific e.g., "The NSTC ML/AI subcommittee should designated a standards coordinator". Others are clearly actions but are non-specific e.g., "Grow a cadre of Federal staff with the relevant skills and training, available to effectively engage in AI standards development in support of U.S. Government interests."	
17	MITRE Corporation	Minor	Page 22, Line 655	Missing reference	Add language regarding the efforts of ASTM's Administrative Committee 377, Autonomy Design and Operations in Aviation. "ASTM Administrative Committee 377, Autonomy Design and Operations in Aviation (AC377) was formed in 2017 through the collective actions of four of ASTM's aviation-related technical committees. The purpose of the administrative committee is to help harmonize standards development efforts related to autonomy/AI in the aviation community. In June 2019, ASTM published a technical report entitled "Autonomy Design and Operations in Aviation: Terminology and Requirements Framework" to serve as a guide for terminology and requirements for increasingly autonomous and complex aviation systems. The committee is now working on technical guidance regarding specific aspects of AI/autonomy to assistant technical committees with their standards development efforts.

18	MITRE Corporation	Major	General	Under-addressed topics within the Plan include: • Development assurance • Partitioning of functionality at multiple levels of criticality • Dynamic data and consistency checking • System and functional modularity • Run-time safety assurance • Fail functionality and high-level redundancy • Human-machine teaming	