Document Title and SDO/Lead Organization: Plan for Federal Engagement in Developing Technical Standards and Related Tools - NIST

Review Due Date: 7/17/19

POC and Component: Jennifer Vallone/Phil Mattson; S&T

Comment #	Section or Page	Comment	Reviewer Component	Reviewer Name
1	p. 9, line 182	after "adoption" add "and maintenance"	PRIV	
2	p.9, line 195	after "use" add "that includes assessments on whether specific data is necessary for processing, the risk to individuals, and how those risks are mitigated."	PRIV	
3	p. 9, line 198	after "technologies." Add new sentence "The tools must support the regular monitoring, evaluation, and auditing of safeguard effectiveness."	PRIV	
4	p. 9, line 200	add new bullet to read: • ***Maintenance of written records of AI system activities*** addressing the purposes and legal basis for processing. Written records should also address third party transfer or usage of data by third parties, applicable notice procedures pertaining to the third party transfer as well as how data integrity and confidentiality is ensured.	PRIV	
5	p. 9, line 211	after "traceability," add "up to date data audits, and data mapping in order"	PRIV	
6	p. 9, line 212	add new bullet to read: "Strategy for maintaining workforce or human resources with appropriate skill sets to monitor, maintain, and optimize use of AI technologies.	PRIV	
7	p. 9, line 213	add 2 new bullets to read: • ***Regulatory requirements*** must be built into the AI system to facilitate compliance with privacy and data protection authorities, as well as obligations to report and remediate data breaches. • ***The ability to restore availability and access*** to personal data in a timely manner in the event of a physical, technical or legal incident or mandate.	PRIV	
8	p. 11, lines 275-276	strike last sentence and replace with "Ultimately, system owners are responsible for ensuring that they take all necessary measures to comply with the law and document both the system's as well as their own compliance."	PRIV	
9	p. 16, line 441	after "deploying" add "and maintaining"	PRIV	
10	p. 7, line 150	in keeping with the requirements of the EO, we would flag the important considerations of risk management, privacy, civil rights and civil liberties	CRCL	

		compliance in AI applications, with the following edit (in italics): "Other aspects, such as trustworthiness, *risk management frameworks, and incorporating privacy, civil rights and civil liberties protections (where applicable),* are only now being considered, if at all."		
11	p. 8, fn. 12	To convey what is expected by the term "risk management," the below text should be included in the footnote, or in a nearby position in the text: "Governance of AI that will perform or support sensitive or complex tasks should also be subject to formal enterprise risk management processes to identify and mitigate compliance issues associated with adoption of the technology. The issues likely to arise may be based in technological, legal, policy, operational, financial, or optics requirements or a blend of any of these and other factors depending on the business processes to be automated, the nature of the AI technology used, and the organization adopting the technology. See, e.g. the *OMB Playbook: Enterprise Risk Management for the U.S. Federal Government*, July 29, 2016."	CRCL	
12	p. 11, line 275	We should convey a lesson learned about how to automate business processes here and state the following about governance to make this section stronger: "Although AI governance is in its infancy, the adoption of AI to supplant or supplement operational activities can be made easier by establishing a governance team that includes subject matter experts in the business process being automated and their associated compliance team. In compliance-sensitive contexts, this may help ensure that applicable compliance principles are appropriately incorporated into both the technology and the policy governing its human users."	CRCL	
13	p. 14, line 366	Add protections for civil rights and civil liberties as part of the ethical requirements because they are applicable to government users of AI and for some private sector users who are subject to Federal civil rights laws (e.g. banking industry, higher education, housing industry, etc.): "… provisions that protect privacy, *civil rights and civil liberties (where applicable),* and reflect the broader community's notions of acceptability."	CRCL	
14	Line 4	Please remove the second "is" for clarity.	CISA/NRMC	Russ Vane
15	Line 34 ff	It is confusing how the country is served by establishing "Technical standards will provide agreed upon language and frameworks" – this is seldom the case with major players contending that AI is <place their tech buzzwords here.> Instead NIST should concentrate on what the EO	CISA/NRMC	Russ Vane

		says – what such innovative commercial players forget is to earn public trust by: *"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; and develop international standards to promote and protect those priorities."*		
16	Line 49	Please replace "learn" with "modify their algorithms better than classical programming techniques"	CISA/NRMC	Russ Vane
17	Line 61 ff	This is an excellent starting list (accuracy, reliability, robustness, security, explainability, safety, and privacy") of the attributes that should increase trust. NIST has an important role here.	CISA/NRMC	Russ Vane
18	Line 74	It is questionable that standards promote "product differentiation and technological innovation"… Invention of new techniques is often the result of relaxing an agreed to "standard practice."	CISA/NRMC	Russ Vane
19	Line 80 ff	A very good point that can be made even more understandable by pointing out that the motivation of AI providers may relax security, safety and privacy standards unless NIST ensures they are available. *And that such providers may be held accountable for such lapses.*	CISA/NRMC	Russ Vane
20	Line 102	"timed too late" is a tautology – please consider another concept such as: "delayed in such a way that"	CISA/NRMC	Russ Vane
21	Line 123 ff	These three lines are very well thought out… more may be needed to convey the deepness of these thoughts to others. Suggestions include: *Preventing errors where all of the pieces work, yet the system fails because of context assumptions during design.*	CISA/NRMC	Russ Vane
22	Line 142 ff	Do we say that these standards should be testable?	CISA/NRMC	Russ Vane
23	Line 173	Note that this document talks about accuracy, security, etc. which are not being addressed. It is likely that the AI providers will have difficulty in trying to objectify their uncertainty. Please remember that AI substitutes "Search for knowledge" in every algorithm. So specific data is important for tuning and approximating completeness. Weak data leads to a bad fit.	CISA/NRMC	Russ Vane
24	Footnote 13	Privacy standards should not be about AI. They should be incorporated in AI.	CISA/NRMC	Russ Vane
25	Line 189	Tools about "reasoning with AI" are similar in scope to serious DoD simulations – verification is	CISA/NRMC	Russ Vane

		tough, validation is almost impossible – in my experience.		
26	Line 195	"parameters of use" should be expanded to context variables which mediate, moderate, and exhibit significant effect size.	CISA/NRMC	Russ Vane
27	Line 209	Remove "good" and replace with "which represent the dependencies exhibited in the domain."	CISA/NRMC	Russ Vane
28	Lines 268-272	Excellent to bullet these two items. No one should disagree that human safety and privacy should be paramount in US IT. It is likely that the illiberal (China, etc.) powers will not be so inclined.	CISA/NRMC	Russ Vane
29	Line 285	"regardless of resources." Please clarify that NIST should provide some support for stakeholders who will be important to AI effectiveness even though they're not the kinds of people usually included in industry-oriented standards committees. *This is extremely important because diversity in AI may prevent axiomatic rigidity that will undermine trust.*	CISA/NRMC	Russ Vane
30	Line 299	The admonition to "avoid standards becoming non-tariff trade barriers" – is questionable. It could very well be unsafe to allow certain kinds of AI into the US based on NIST's wise understanding of accuracy, safety, security, etc. Please rethink.	CISA/NRMC	Russ Vane
31	Line 322	"nimble" is just "agile" in another form. Not all standards should be "come as you think of it." Security often cannot be a last minute addition.	CISA/NRMC	Russ Vane
32	Line 341	Poor definition of innovation – rethink as a novel representation that doesn't just improve a process – that's product/process improvement – it's when one considers several possible future contexts and finds a jump-shift, which is a change in process that will cause or exploit a change in context.	CISA/NRMC	Russ Vane
33	Lines 339-340	Please don't start with an excuse. The list that follows should have a rough prioritization, and the texts should be more substantive. This looks like a late addition that does not have the careful thought of previous sections. If needed, collapse the list into four larger categories with these as examples of instances to prioritize.	CISA/NRMC	Russ Vane
34	Lines 367-368	This is rote. Is there anything that complex adaptive systems might do to confound these? If not why not?	CISA/NRMC	Russ Vane
36	Lines 447-449 (bold)	Well said. And on point. Gentle reminder – AI must radically change in the next four years because of the collapse of Moore's conjecture – processors are not faster – don't let Nvidia (or any SIMD processor) fool you.	CISA/NRMC	Russ Vane
37	Line 521	AI has about 50 definitions – include a bunch of them here as a testimony to the difficulty of this work.	CISA/NRMC	Russ Vane

		Perhaps John McCarthy's original is best, but it will generate a howl in the industry. AI will have a renaissance if NIST does this work well. Here's the point tactical data-searching algorithms look great on toy problems, but the combinatorics will kill the field (see algorithmic complexity). It is likely that China will not understand this and invest in the wrong things. *The key is the invention of new abstractions that leap past OWL and current ontological representations – see Poythress* On Ontology. The US inventors can and will do this.		
38	p. 15, Footnote 24	Typo: "Usining utandards" should be "Using Standards"	All DHS	
39				

Acronyms:

- CISA NRMC – US Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, National Risk Management Center
- CRCL – US Department of Homeland Security Office for Civil Rights and Civil Liberties
- DoD – US Department of Defense
- EO – Executive Order
- IT – Information Technology
- OMB – US Office of Management and Budget
- OWL – W3C Web Ontology Language
- PRIV – US Department of Homeland Security Privacy Office
- SIMD - Single instruction, multiple data