GEMMA AUGUSTO, M.S.
IA Engineer
Augusto95@aol.com

June 09, 2019

The Honorable Walter G. Copan, PhD
Under Secretary of Commerce for Standards and Technology
U.S. Department of Commerce
National Institute of Standards and Technology
100 Bureau Drive, Stop 2000
Gaithersburg, Maryland 20899

Re: NIST RFI: Developing a Federal Artificial Intelligence Standards Engagement Plan
Docket No.: [190312229-9229-01]

Dear Dr. Copan:

The U.S. should take an open and global approach in developing policies and guidance to facilitate research and collaboration in AI across the globe. A global AI standard will enable a global AI terminology, interoperability and scalability of AI software code, algorithms, architectures and ecosystems. The world will become a better place with the fusion of knowledge and technologies. For instance, data sharing must be done following global laws and security principles in order to facilitate cross-border data flow and prevent lawsuits. Organizations and the private sector must provide individuals with privacy notices as an individual's private data might be collected for medical and other types of research. Countries should comply with source code disclosure license and confidentiality agreements when sharing data for AI research, programs, and projects. Security principles must be in place from the data acquisition process through the AI architectures and lifecycle in order to better manage security risks such as data privacy, insider threats, and bugs in the code. For instance, data sharing should be encrypted and software code should be written with security across the lifecycle. In addition, a rotation of duties and an effective secure identity management solution should be in place to minimize the possibility of collusion and insider threats through the process of an AI technology lifecycle, especially with regard to R&D in the DHS, DoD, and Intelligence arena.

As Artificial/ Augmented Intelligence is still in its infancy and there is still a lot of ongoing research in many different disciplines, the future of an AI lifecycle and AI Architectures will be very complex. The Artificial / Augmented Intelligence lifecycle must include a hybrid approach as many other technologies are and will be combined. Areas of consideration to take into the account of the AI's lifecycle are other technologies such as 5G, IoT, and cloud computing, just to name a few, as these technologies will fuse; a hybrid approach of not just other technologies as mentioned above but also secure algorithms (e.g. neural networks are vulnerable to adversarial examples), and secure software code; a data center of excellence; data acquisition and data sharing following global laws; security across the lifecycle and architectures; interoperability, scalability, functionality, and ethics (including unbiased algorithms); trustworthiness (verification & validation) of an AI solution; AI metrics; AI certification and approval; continuous security monitoring; and human oversight across the AI lifecycle since AI technologies lacks human intuition, emotions and deductions, could give false positives and false negatives, and data/software/algorithms/hardware upgrades/uploads need human verification and validation.

An AI technology should be developed and used to help humans and only humans should have a final decision when using AI technologies as an AI technology lacks human intuition, feelings and deduction. For instance, an AI technology in image recognition in an MRI might get false positives or false negatives and it could be a decision between the life and death of a patient. Furthermore, the AI patient's medical records might not have all the patience's medical information. AI technologies should be implemented to aid doctors and health practitioners to make a better diagnosis and the doctor should have the final decision. The same principle is applicable in the role of AI in the future of warfare and autonomous systems.

An AI technology might need data upgrades, software and algorithm modifications as well as hardware changes and upgrades and certification and approval. Furthermore, an AI technology could have a defective sensor or device and could have catastrophic consequences. Therefore, there should be a regulatory framework across the board for modification in AI technologies as data might need to be updated and software code and algorithms need to be modified. This is true for example in medical devices.

Organizations and the private sector must have precautions when deciding to implement an AI Technology. A hybrid approach of an AI technology and human collaboration might be the best solution. An AI technology is as good as its design, implementation and continuous monitoring by humans. All the factors above should be taken into consideration when developing AI standards.