AI RFI Responses, October 26, 2018

Update to the 2016 National Artificial Intelligence Research and Development Strategic Plan RFI Responses

DISCLAIMER: The RFI public responses received and posted do not represent the views and/or opinions of the U.S. Government, National Science and Technology Council (NSTC) Select Committee on Artificial Intelligence (AI), NSTC Subcommittee on Machine Learning and AI, NSTC Subcommittee on Networking and Information Technology Research and Development (NITRD), NITRD National Coordination Office, and/or any other Federal agencies and/or government entities.
We bear no responsibility for the accuracy, legality or content of all external links included in this document.

ISACA®
1700 E. Golf Road, Suite 400
Schaumburg, Illinois 60173, USA
Telephone: +1.847.253.1545
isaca.org | E-mail: info@isaca.org

Response to Request for Information on Update to the 2016 National Artificial Intelligence Research and Development Strategic Plan

Document: 83 FR 48655
Document Number: 2018-20914

ISACA, on behalf of its nearly 60,000 information and cyber security professionals in the United States and its global community of nearly 140,000 professionals, is grateful for the opportunity to provide comments on the National Science Foundation's Update to the 2016 National Artificial Intelligence Research and Development Strategic Plan.

The Update to the 2016 National Artificial Intelligence Research and Development Strategic Plan is both timely and welcome. While the strategic aims of the Update are well-crafted, there are several elements that ISACA believes deserve additional consideration and potential action:

Strategy 3

The Update notes the need for accountability-by-design; ISACA agrees strongly with this approach, as well as the foundational emphasis it is being given. In addition to the requirements outlined in the Update, however, ISACA believes that there is a need for machine learning and artificial intelligence (ML/AI) audits, process audits for contractors, and potentially full algorithmic audits for governmental agencies. For both process audits and full algorithmic audits, however, the emphasis must be on audit activities that ensure the process for creating algorithms is controlled and does not require the disclosure of intellectual property or other elements of a proprietary nature.

In addition, ISACA would also respectfully suggest the inclusion of a robust control framework, along the lines of the NIST Cybersecurity Framework, be put in place. There are already organizations pioneering work in algorithmic audit, and these possibilities should be explored as well. Likewise, approaches for process auditing can be found in ISACA's own CISA certification coursework, as well as the curriculum of any number of IT Audit-focused certifications currently in use today. ISACA believes that incorporating an overall focus on audit within ML/AI is very much in keeping with the concepts of accountability-by-design that are put forth in the Update.

Strategy 4

The Update's focus on securing the embedded ML/AI in critical systems is a welcome approach, and ISACA shares the Foundation's belief that such efforts will be essential moving forward. ISACA would also respectfully suggest the inclusion of a control framework for testing systems for resistance to adversarial attacks.

Strategy 5

While ISACA agrees with the Update's emphasis on the need to develop shared public datasets and environments for ML/AI training and testing, as well the Update's additional support for data pre-processing techniques such as data cleaning, we believe the Update could go further in this regard. ISACA believes that a framework and controls for data quality standards should be put in place. With such a tool in place, ISACA believes the Foundation's goals (ensuring that any form of discriminatory bias does not exist within datasets; that the data itself is of the highest quality, etc.) could be more readily and sustainably met going forward. In ISACA's considered opinion, ensuring the quality and effectiveness of any shared public datasets and environments for AI training and testing is a crucial governance task. As these datasets change and evolve, so will the algorithms that are associated with the datasets. It is critical that governance exists that ensures these tools continue to meet internal and external requirements, and are subject to ongoing monitoring, review and, when necessary, remediation. Absent such governance, these shared datasets and environments run the risk of failure. Even with such governance present, measures should be put in place so that if and when negative effects do occur, they can be dealt with swiftly, before their impact widens.

Strategy 6

In Strategy 3, the Foundation expressed its staunch support for accountability-by-design, and ISACA believes that same focus should be employed in driving the use of standards and benchmarks to measure and evaluate ML/AI technologies. Adherence to tools such as risk-based audits, as opposed to 'check-the-box' compliance to regulations or laws is, ISACA contends, more beneficial to ensuring that accountability, security and integrity are foundational elements of any efforts within ML/AI technologies. ISACA believes that incorporating such risk-based audit strategies in an ML/AI environment, echoing the compliance of internationally-recognized audit standards, is the best way to ensure ML/AI technologies and systems remain protected and governed by recognized and established controls.

ISACA's review of the Update also includes one area in which we believe the Update could take better advantage of an opportunity it has presented. The Introduction to the Update poses several questions regarding the appropriate role of Federal investment in the development of ML/AI technologies. One of the questions posed is: *Are there opportunities for industrial and international R&D collaborations that advance U.S. priorities?* This question, in ISACA's considered opinion, raises a key concern that is only glancingly addressed in the Update and, we believe, deserves additional consideration and focus.

If government and industry collaborate, a balance must be struck between the need for transparency on government's part, and the desire on industry's part for proprietary advantage (i.e., proprietary algorithms, analytic software, data structures, etc.) to be maintained. For this reason, ISACA believes that, in any government and industry collaboration, additional emphasis should be placed upon the auditing, governance and risk management of the processing of data within the ML/AI environment, and that those efforts also be held to internationally recognized standards, frameworks, and benchmarks.

Strategy 7

ISACA shares the Foundation's concern for predicting future workforce needs, including pipeline issues such as educational pathways and re- and up-skilling opportunities, as well as the need for diversity and inclusion. Though there is a definite need to better understand the national ML/AI research and development workforce needs, ISACA believes that the strategy outlined in the Update could benefit from an additional focus on the need for a 'translational' corps of professionals to ensure there is a clear path from exceptional research to the application of that research. It is critical that the technology transfer between ML/AI researchers and professionals in the public and private sectors occur seamlessly. It is ISACA's belief that such efforts would be of great benefit to rounding out the capabilities of an effective, efficient, and forward-focused ML/AI workforce.

Thank you again for this opportunity to share ISACA's perspectives on the National Science Foundation's Update to the 2016 National Artificial Intelligence Research and Development Strategic Plan. ISACA looks forward to working with the National Science Foundation and the Federal government as the Strategic Plan moves forward.