AI RFI Responses, October 26, 2018

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

26 October 2018

Attn: Faisal D'Souza
Networking and Information Technology Research and Development (NITRD)
National Coordination Office (NCO)
National Science Foundation
2415 Eisenhower Avenue
Alexandria, VA 22314

Via Email: AI-RFI@nitrd.gov

Re: RFI Response: National Artificial Intelligence Research and Development Strategic Plan

IEEE-USA is pleased to submit these comments on the above-captioned, *Request for Information on Update to the 2016 National Artificial Intelligence Research and Development Strategic Plan* (83 FR 48655).

IEEE-USA represents approximately 180,000 engineers, scientists, and allied professionals across the United States, many of whom are actively conducting research and development into artificial intelligence cybersecurity, IoT, advanced computing as well as other foundational and emerging technologies. We are the American component of the IEEE – the largest organization of technology professionals in the world, representing more than 450,000 engineers, scientists and allied professionals worldwide.

IEEE-USA believes that an artificial intelligence national strategy is essential for the country and that the US government has a central role in promoting innovation and responsible governance, and mitigating the potential risks and challenges of implementing emerging technologies. In 2016, IEEE-USA published, "*Artificial Intelligence Research, Development and Regulation*"[1] and the IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems published the evolving, *Ethically Aligned Design: A Vision for Prioritizing Human Well-Being with Autonomous and Intelligent Systems*.[2] IEEE is also developing technical standards that offer an extensive framework to prioritize ethical considerations in the design, development, and deployment of autonomous and intelligent systems (A/IS).[3]

We believe that any national strategy for AI must be one that guarantees successful and ethical R&D, as well as public acceptance of AI systems. At the same time, we must not overregulate or inhibit private sector innovation. Accordingly, we wish to provide the following recommendations drawing on our collective expertise in line with the goals of the RFI.

1. Ensure that an understanding of the impact of AI on individuals and society at large is central to AI R&D strategies so as to promote public acceptance of AI.

---

[1] https://ieeeusa.org/wp-content/uploads/2017/10/AI0217.pdf

[2] https://ethicsinaction.ieee.org/

[3] https://standards.ieee.org/content/dam/ieee-standards/standards/web/documents/other/ead_v2.pdf

IEEE-USA believes that the *National AI R&D Strategy* should promote the concepts of "accountability," "transparency," "explain-ability," and "fairness" by encouraging public input and engagement. A national strategy that reflects the concerns and thoughts of a broad representation of academia, the standards development community, labor, civil society, as well as businesses and industry, will ensure long-term success, mitigate risks, and promote public acceptance.

Artificial intelligence presents complex public policy challenges, including societal and economic implications (labor shift, skill demand, the future of work, and societal structures and norms), safety, security, and data privacy. A key challenge of the knowledge-based economy will be preventing the situation where technology development occurs in silos and only the few who possess the technical knowledge make decisions impacting the interest, rights, and livelihood of the many. Including broad representation of the non-tech community could help bridge these sharp cultural divides and preserve individual rights.

Policymakers, economists, and researchers must look at the speed of technological disruption, its implications on the market and governing institutions, and the speed at which subsequent adjustments takes place. Undoubtedly, the speed of AI disruption will influence consumer demand, market inertia, pricing models, overhead cost, and other microeconomic and macroeconomic factors. These factors themselves vary greatly from one part of the economy to another. Technological disruption may have a tangible influence on the public interest, including statutory and constitutional rights.

Internationally recognized legal norms like the *United Nations Guiding Principles on Business and Human Rights*, also known as the Ruggie Principles, offers a framework that guides AI R&D and could ensure that American technology is superior, more competitive, and universal. The priority principles are:

- **Responsibility**: Identify right holders and duty bearers, and ensure that duty bearers have an obligation to fulfill all human rights.
- **Accountability**: As duty bearers, states should be obliged to behave responsibly, seek to represent the greater public interest, and be open to public scrutiny of their A/IS policy.
- **Participation**: Encourage and support a high degree of participation from all interested parties.
- **Non-discrimination**: Principles of non-discrimination, equality, and inclusiveness should underlie the practice of A/IS, with particular focus given to vulnerable groups, such as minorities, indigenous peoples, and persons with disabilities.
- **Empowerment**: Right holders must be able, and encouraged to exercise their rights.
- **Corporate responsibility**: Companies must ensure that their A/IS comply with the rights-based approach. Companies must not willingly provide A/IS technologies to actors that will use them in ways that lead to human rights violations.

Furthermore, we recommend removing impediments to research on the fairness, security, privacy, and social impacts of AI systems. Some interpretations of Federal laws, such as the Computer Fraud and Abuse Act (CFAA) and the anti-circumvention provision of the Digital Millennium Copyright Act (DMCA) are ambiguous regarding whether and how proprietary AI systems may be reverse engineered and evaluated by academics, journalists, and other researchers. In some cases, the interpretations of federal laws have made illegal in cyberspace what has long been legal in physical space. Researchers

and other outside parties must be permitted to evaluate and test AI systems to protect public safety and encourage public acceptance of new technologies.

Finally, regarding the discussion of workforce in Strategy 7, IEEE-USA recommends establishing a partnership between the US Census Bureau and the US Bureau of Labor Statistics to study the effects of adoption of AI and AI-related technology on the US workforce. The data could help answer multiple questions regarding direct and indirect impacts, including (1) how AI affects firm-level productivity; (2) which types of firms are more likely to invest in AI; (3) the extent to which AI is complementing or substituting human labor; and (4) how market structure affects a firm's incentives to invest in AI.

2. Prioritize long-term, high-risk, high-reward research and increased federal investments in all areas of AI.

The current *National AI R&D Strategy* stresses that greater federal investment in programs dedicated to AI R&D is critical to maintaining U.S. competitiveness in this field. Much of the US government's dedicated AI research is taking place within agencies comprising the NITRD consortium, specifically within the RIS (Robotics and Intelligent Systems) Program. Since the *National AI R&D Strategy* was published in 2016, multiple AI-focused programs have been established in the DoD – e.g. the Joint Artificial Intelligence Center and DARPA's "AI Next." IEEE-USA recommends that the administration's 2020 budget proposals include similar strong investments in non-defense AI research and development. For example,

- Doubling the NITRD's RIS budget in FY 2020 with a target of $1 billion in 5 years and distributing it among contributing members of the program: DoD, NSF, NASA, and NIST.
- Significantly increasing the budget for NSF CISE in FY 2020, with significant annual increases for at least five more years. CISE has an impressive track record of identifying and funding early research that led to the Google search algorithm, among many other feats.
- Prioritizing investments in high performance computing (HPC) which will accelerate the progress of AI. HPC programs include: Enabling R&D for High-Capability Computing Systems (EHCS) and High Capability Computing Infrastructure and Applications (HCIA), both within NITRD, High Productivity & High Performance Responsive Architectures in ITC at DARPA and Advanced Scientific Computing at DOE.

NITRD's RIS, NSF CISE, DoD RDT&E and DOE Advanced Science Computing are all poised to focus research on the fundamentals of AI and data-intensive theories and applications, high performance and supercomputing, novel computer architectures like neuromorphic computing and novel semiconductor materials. This research will enable faster and more powerful artificial intelligence computing. We believe that these programs should devise research projects that prevent cognitive biases of human administrators and unintentionally inferred biases from extending to AI.

Further, the *National AI R&D Strategy* should prioritize long term high-risk/high-reward research in all key next generation opportunities for AI. IEEE-USA recommends:

- Robust AI: Study and research of resilient AI systems capable of withstanding malicious, cyber and adversarial attacks. Develop proper AI defense technologies to ensure public safety, in addition to reliable and fail-safe AI.

- High Performance AI: AI specific high performance, low power hardware design, AI accelerated hardware design, and more efficient and faster machine learning algorithms.
- Explainability and verification of deep neural networks via model validation, evaluation protocols, transparency and measurement standards.
- Ethical AI: Research into creating fundamental and new formal and normative modeling techniques for embedding ethical principles in autonomous systems and into building AI that mirrors human ethical behavior, societal norms and values.
- AI for Cybersecurity and for countervailing the potential disastrous impact of technologies like deep fakes.
- Cross domain and interdisciplinary medical AI: Research and development of precision medicine, drug discovery, and genetic research.
- Next Generation AI: New machine learning theories that understand cause and effect and context, not just correlation in data.

Finally, IEEE-USA believes that building strong scientific and diplomatic relationships with key U.S. allies that are assuming a leadership role in AI research and governance, such as Canada, the UK, Japan, France, South Korea, and Germany, should be a key goal of the strategy. The Department of State (Office of the Science & Technology Adviser) should lead this effort.

3. Prioritize protecting U.S. Intellectual Property by advising the Department of Commerce and other agencies on emerging technologies.

IEEE-USA believes the *National AI R&D Strategy* should reflect the current legal environment governing export control measures and the foreign investment risk review process intended to protect U.S. intellectual property. Protecting U.S. intellectual property from theft – costing an estimated $300 billion per year –via cyber espionage or acquisition by economic rivals is vital to the U.S. national security, innovation, and the economy.

We believe that any advisory body tasked with regulating federal AI policy should be a part of the ECRA interagency process and the CFIUS process, and should advise both the Secretary of Commerce and Secretary of Treasury on AI and constituent technologies to better protect US intellectual property.[4]

Strategy 3 of the *National AI R&D Strategy* addresses legal issues but not from an intellectual property perspective. For instance, AI disruption of patent subject matter, inventorship (i.e. can a machine be considered to be an inventor for a specific applicable algorithm) and/or liability and infringement (i.e. the question of legal liability if a competitor's machine generates/executes a sufficiently close algorithm). Moreover, we also believe that personal data rights of users providing data for any AI system should also be considered in regard to assignment of intellectual property rights for appropriate compensation, control, or

[4] The Export Control Reform Act of 2018 (ECRA) establishes a new formal interagency process at the Department of Commerce to identify and impose additional controls on emerging and foundational technologies that are essential to U.S. national security, particularly with respect to potential threats from economic rivals. Said technologies are likely to include areas such as artificial intelligence, robotics, augmented reality or virtual reality, and financial technology. In enforcing ECRA provisions, the Department of Commerce consults with other agencies (Defense, Energy and State) to identify and provide advice on emerging and foundational technologies requiring control. Additionally, the Foreign Investment Risk Review Modernization Act (FIRRMA) establishes at the Department of Treasury, additional requirements for investigating joint ventures to ensure transparency of the arrangements and their participants; and expands the jurisdiction of the Committee on Foreign Investment in the United States (CFIUS).

ownership of that data.

4. Promote and facilitate the use of AI in government services, and improve government expertise in AI and emerging technologies.

IEEE-USA calls for a defined path towards increased AI technical expertise within the U.S. Government workforce, and increased government access to private-sector technical expertise to ensure sound public policies and regulations. This recommendation concurs with the multiple recommendations of the National Science and Technology Council's publication, *One Hundred Year Study of Artificial Intelligence*, that more technical expertise is required to create a public policy, legal, and regulatory environment that allows innovation to flourish while protecting the public.

Executive branch agencies should create pilot programs to examine how each of the seven strategies of the *National AI R&D Strategy* will work best in practice so that eventually they can be implemented broadly. The programs could include examining how to improve AI R&D workforce development, establishing safety and security standards, and benchmarking health care information, etc.

So as to not negatively impact private industry, these pilot programs could focus on agencies that are inherently federal government operations: Department of Justice (algorithms in criminal justice), National Highway Transportation Safety Administration (autonomous vehicles), and National Transportation Safety Board (safety investigations and analyses of autonomous systems). Each of these agencies has their own unique concerns and opportunities for use of AI, and administration oversight can facilitate agency use and development.

With at least 16 different agencies currently governing sectors of the economy related to AI, uniformity may be difficult to achieve. Thus, to ensure consistent and appropriate federal AI use and regulation, IEEE-USA calls for creation of an interagency panel to coordinate federal activity. The interagency panel should seek expert input from stakeholders, including those from academia, standards organizations, and industry, to consider questions related to the governance and safe deployment of AI. Specifically, the panel should make recommendations on societal implications, public engagement, appropriate levels of investment, economic and national security impacts, trust and safety assurance, and other legal and regulatory matters. As a well-respected agency, the National Institute of Standards and Technology would be an effective panel lead.

We also recommend establishing new permanent offices and positions with a specific focus on AI technical expertise (e.g. U.S. Digital Service and ARPA-ED), and providing more support for programs that temporarily place technical experts within government (e.g. academic personnel under the Intergovernmental Personnel Act, Presidential Innovation Fellows, and the Science and Technology Policy Fellows program).

5. Strengthen transfer and commercialization of emerging technology from federal labs.

Through a variety of technology transfer vehicles, including licensing, cooperative research and development agreements, the private sector develops and commercializes remarkable cutting-edge research that originates in government laboratories and Federally Funded Research & Development Centers. The new products and services conceived by federal research significantly contribute to the

nation's economy and often provide solutions to pressing national needs.

IEEE-USA believes that updates to the *National AI R&D Strategy* should prioritize identifying policies, regulations, and best practices to address the systemic challenges to effective tech transfer of AI. Barriers to tech transfer include high transaction costs and inconsistent rules and processes across federal agencies.

Any designated advisory body tasked with coordinating and/or regulating federal AI policy should collaborate with NIST to actively communicate to individuals and businesses with interest in transferring technology, perhaps using tools such as technology open-houses and regular stakeholder roundtables. The advisory body could also work with the Office of Advocacy in the Small Business Administration to help entrepreneurs navigate the landscape of technology transfer processes, licensing issues, and other legal matters.

In conjunction with facilitating tech transfer, IEEE-USA believes that the *National AI R&D Strategy* should promote the creation of business incubation models, such as the DoD Defense Innovation Unit (DIUx), within other executive agencies to provide non-dilutive capital in exchange for commercial products that advance its strategic national goals. DIUx successes include subsequent private venture capital investments in start-ups that help the U.S. military make better use of emerging commercial technologies. These incubators have strong potential for attracting and developing human talent, and promoting the growth of entrepreneurial ecosystems and business clusters around the country.

6. Create national academic centers of excellence for developing a workforce skilled in AI.

IEEE-USA recommends the creation of national academic centers of excellence, focused on skill acquisition and apprenticeships. To satisfy the need for exceptional talent to conduct cutting edge AI research, and to ensure a well-qualified workforce for AI deployment into the economy, IEEE-USA believes we need a new model for agile technical education that focuses on experiential co-learning and on-the-job training. Community colleges can play a significant role in bridging the talent and skills gaps by attracting a larger constituency to fill tech jobs, including in AI. Current successful examples of this collaborative model between community colleges and universities have been implemented in Massachusetts (Massachusetts Technology Leadership Council) and Virginia (Northern Virginia Community College - NOVA), and have proven to be successful.

NOVA succeeded in scaling up their offerings in applied and associate degrees, in being one of the first Certified Academic Excellence programs in partnership with the NSA, and offering complete bachelor degrees to their students in conjunction with nine universities. NOVA also successfully partnered with the United States Marine Corps and the Marine Corps University to offer to transitioning servicemen/women and veterans, placement in technology boot camps and affordable cybersecurity programs. It launched an apprenticeship model with Amazon Web Services to certify Amazon employees on cloud security, and succeeded in reaching out to high schools and underrepresented minorities and women in STEM. These efforts could be replicated across the country.

This recommendation is in line with the *Strengthening Career and Technical Education for the 21st Century of 2018 Act* which allows the states to dedicate additional resources for community colleges and other educational institutes for high-demand fields such as cybersecurity and artificial intelligence

based on changing economic, educational, or national security needs.

IEEE-USA thanks NITRD for considering these comments in the agency's revisions to the *National Artificial Intelligence Research and Development Strategic Plan*. We would welcome any further discussions with the agency on these matters. If you have questions, please do not hesitate to contact Erica Wissolik at (202) 530-8347 or e.wissolik@ieee.org.

Respectfully submitted,

Sandra L. Robinson
2018 President, IEEE-USA