Request for Information to the Update of the National Artificial Intelligence Research and Development Strategic Plan: Responses

State University of New York Canton

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government or any entity within the U.S. Government. We bear no responsibility for the accuracy, legality, or content of the responses and external links included in this document.
March 3, 2022

RE: RFI Response: National Artificial Intelligence Research and Development Strategic Plan” in the subject line of the message.

Dear Office of Science and Technology Policy,

The Advanced Information Security and Privacy (AISP) Research Lab is housed at The State University of New York in Canton and is the hub for national and international collaboration on research and education efforts on Information Technology and Artificial Intelligence. The AISP Lab has more than 16 Research Fellows, Graduate and Undergraduate students, visiting scholars and has helped over 30 members with their Doctorate dissertations, Masters’ theses and Internship projects over the years. The AISP Lab is the focal point for not only the State University of New York’s CyberSecurity program, but also a place for our community to educate and enhance their knowledge of AI and CyberSecurity. More information can be found at: www.ghazinour.com/AISP

The AISP Lab respectfully submits its comments on THE NATIONAL ARTIFICIAL INTELLIGENCE RESEARCH AND DEVELOPMENT STRATEGIC PLAN as follows below.

Upon review of the 2019 plan in light of recent events, we request the Government prioritize the following three areas for immediate, robust and sustainable focus and funding:

A. **Strategy 4: Ensure the Safety and Security of AI Systems**
   1) **Securing against attacks.** With conflicts rising globally and the high-stakes of AI and cyberspace infrastructure, protecting and defending our AI systems is not a luxury option but an immediate need.
   2) **Autonomous attack analysis and countermeasures.** Expand on DARPA’s efforts that “involved AI agents autonomously analyzing and countering cyber-attacks” (p. 26) Although major targets such as government agencies, and sensitive major businesses already benefit from sophisticated and costly existing autonomous systems, we would like to emphasize that we strongly believe such autonomous systems should be widely available and affordable for others to ensure that universal, accessible and responsive AI agents protect a wide array of traditionally underprepared potential targets, including:
      - Health care providers
      - Small to mid-size financial institutions
      - First responders
▪ Small businesses
▪ Industries involved with cyber-infrastructure
▪ K-12 schools
▪ Local governments
▪ Faith communities
▪ “Last mile” grid/infrastructure providers
▪ “First mile” food providers – especially farmers

B. Strategy 5: Develop Shared Public Datasets and Environments for AI Training and Testing
   1) Making training and testing resources responsive to commercial and public interests (p. 34)
      ▪ Expand efforts similar to DHS IMPACT program which “supports empirical data sharing between the international cybersecurity R&D community, critical infrastructure providers, and their government supporters” ideally with “dynamic, agile repositories” with the broadest view of infrastructure to ensure agility in data collection, analysis and responsiveness to diverse interests of industry and citizenry adrift and drowning in a sea of unstructured data.

C. Strategy 8: Expand Public–Private Partnerships to Accelerate Advances in AI
   1) Advancing our Nation’s AI innovation ecosystem. The vast subject area of AI and its diverse active players within it is too complex to be only run by the public or private entities separately. The collaboration and partnership between them needs to be expedited and facilitated if we are hopeful to benefit from advancements made by both parties.
   2) Expand Government-industry-University research partnerships that engage efforts to communicate clearly and simply best practices in daily life for cybersecurity to motivate students, employees, warfighters and academics to exchange applied experiences in a rapid, agile and iterative process with researchers to quickly disseminate life-saving AI tools, develop novel, “US-first or best” applications and disarm domestic, foreign and rogue AI threats.

I am happy to report that The AISP Research Lab, The Cybersecurity Program and the Center for Criminal Justice, Intelligence and CyberSecurity with the collaboration of our partners offer:

A. Suggestions for priorities
   a. Investing on research regarding Privacy and Security aware AI systems
   b. AI systems that interact with non-traditional legacy systems such as IoT, pervasive networks and social media platforms

B. Key concerns to address
   a. Ethics in AI is placed as one of our highest key concerns. With the use of advanced AI algorithms, discriminatory and biased algorithms are increasingly available and
it is essential to educate the workforce on basic ethics of using such powerful AI systems.

b. AI-inspired Social Engineering attacks. With the advancement in collecting and analyzing digital footprints from cyberspace users, the adversary can build a system that expertly impersonates individuals and can create a more believable platform to use for social engineering attacks.

C. Aspirations to sustain success
   a. The AISP Research Lab with its successful track record of receiving funds from government agencies ($2.5M since 2019), and a large, collaborative group of research fellows, scholars and students is capable of assisting government agencies and private organizations in proper use of AI-inspired systems in a safe and secure manner.
   b. The AISP lab with over 60 peer-reviewed publications in national and international journals and conferences plays an important role in dissemination of knowledge to empower our community to utilize AI systems with security and privacy in mind.

D. Lessons learned from our work
   We have learned that having the most secure and trusted AI systems are only one piece of the puzzle. The most important piece is to build secure, affordable and user-friendly AI systems that provide utility, security and other benefits to individual users. It has been proven over and over that systems that are secure but introduce a lot of complexity are not effective and they can be counterproductive as they discourage users to engage with the AI systems. An additional risk is that overly complex AI systems can become vulnerable to adversaries using ever-increasing malicious techniques to misuse their data.

E. An invitation to share
   a. The AISP Lab invites the Government to a no-cost platform to promote the AI R&D Plan as a key part of our annual National Cyber Security Month Virtual Symposium – we would be honored to host sessions with a dedicated conference track on the subject so your experts can describe the plan and invite a diverse group of AI experts to join the effort to implement the plan.
   b. The AISP Lab commits to promote the AI R&D plan through alignment with our curriculum to train the next generation of AI researchers, developers, policy makers and entrepreneurs.
   c. The AISP Lab plans to establish a multidisciplinary, applied internship program with SUNY cybersecurity and other students and our Innovation Fellows to help develop and implement the AI R&D plan on a local level with small businesses, K-12 schools, first responders, city government and other traditionally
underprepared sectors as a model to be replicated with universities across the country.

We hope the above points would respectfully assist your office and we are looking forward to our collaboration in building safe and secure AI enabled communities.

Sincerely,

Kambiz Ghazinour, PhD.
Director of the Advanced Information Security and Privacy (AISP) Research Lab
Associate Professor, State University of New York at Canton.