ADVANCING GOVERNANCE, INNOVATION, AND RISK MANAGEMENT FOR AGENCY USE OF ARTIFICIAL INTELLIGENCE (AI):

PROPOSED MEMORANDUM IN RESPONSE TO REQUEST FOR INFORMATION (RFI) RELATED TO NIST'S ASSIGNMENTS UNDER SECTIONS 4.1, 4.5 AND 11 OF THE EXECUTIVE ORDER CONCERNING ARTIFICIAL INTELLIGENCE (SECTIONS 4.1, 4.5, AND 11)

CYBER FLORIDA
at the UNIVERSITY OF SOUTH FLORIDA

CYBER FLORIDA
at the UNIVERSITY OF SOUTH FLORIDA

CYBERFLORIDA.ORG

22 January 2024

National Institute of Standards and Technology:

On behalf of the Florida Center for Cybersecurity, also known as Cyber Florida, I would like to thank you for the opportunity to submit a response to your request for information and address the important issue of advancing artificial intelligence innovation and determining risk management policies.

Cyber Florida was established by statute in 2014 to help position Florida as a national leader in cybersecurity by promoting cybersecurity education, research, and outreach. Hosted by the University of South Florida, Cyber Florida leads a spectrum of initiatives to support industry-advancing research, inspire and educate future and current professionals, and help people and organizations better understand and prepare for cyber threats.

Among our key mission areas at Cyber Florida is to advance cybersecurity research, including that of artificial intelligence, to improve the cyber readiness of the state and Nation. In that regard, we've included several recommendations in this response that we believe will assist in developing a comprehensive plan for agencies regarding the proper use of artificial intelligence and its impact on the rights and safety of the public.

We commend the National Institute of Standards and Technology (NIST) for leading the effort on advancing governance, innovation, and risk management for agency use of artificial intelligence, as we believe this to be of utmost importance in our Nation's continuous fight against cyber threats. Cyber Florida is committed to serving as a resource to help NIST address this issue and others. We remain at your disposal for further discussion.

Respectfully,

General (Ret.) Kenneth F. McKenzie Jr.
Executive Director, The Florida Center for Cybersecurity

4202 E. Fowler Avenue, ISA7020, Tampa, FL 33620-7120 | info@cyberflorida.org | 813 974 2604


MARSHALL
STUDENT CENTER

The Florida Center for Cybersecurity (Cyber Florida)

The Florida Center for Cybersecurity was established within the University of South Florida in 2014 under Florida statute 1004.444. The goals of the center are to: position Florida as a national leader in cybersecurity and its related workforce through education, research, and community engagement; assist in the creation of jobs in the state's cybersecurity industry and enhance the existing cybersecurity workforce; act as a cooperative facilitator for state business and higher education communities to share cybersecurity knowledge, resources, and training; seek out partnerships with major military installations to assist, when possible, in homeland cybersecurity defense initiatives; attract cybersecurity companies to the state with an emphasis on defense, finance, health care, transportation, and utility sectors.

Comment

Artificial Intelligence (AI) is no longer a term associated solely with experts in technology. It has become so common that even children can and are experiencing the impact of AI on their lives, and beyond that, they can comprehend the change AI is enabling today. Applications unimaginable five years ago are now seeing rapid permeance in our society. Humanity has seen nothing equal to the scope, scale and speed of AI advances in

its recent history. The time is indeed now to ensure that mistakes made in the past – a most glaring example is cutting corners in cybersecurity with the development of the Internet and its protocols – are not repeated, and a clear, comprehensive and practical plan for managing AI advances and its associated risk is developed. We are delighted that NIST is taking a leadership role in this regard. Cyber Florida is also eager to contribute its expertise to this effort.

Strengthening AI Governance: We recommend the need for a dedicated Chief AI Officer (CAIO) tasked with the broad oversight of myriad ways in which AI advances might impact the functioning of a governmental agency. Apart from this, a Governing Board that can periodically oversee and advise the CAIO on AI-related topics is highly recommended. In fact, a cursory look across hiring in the C-Suite categories now reveals a growing trend in Chief AI Officers positions in the private sector. We believe that requirements for a CAIO at the Governmental Agency level cannot just be someone with significant technical expertise (AI or otherwise), but instead must be well versed with agency's priorities, understand the complex dynamics of departments within the agency, where opportunities and barriers for AI innovation lie, and understand/identify clear use cases. Most importantly, stakeholders in the respective agencies need to sensitize to the fact that AI may not solve everything (like the perception that advent of Chat GPT has enabled), and hence the CAIO must be someone with a deep understanding of not only the strengths of AI, but also its limitations with-in the purview of each agency. The presence of a formal Governance Board will go a long way in giving a clearer sense of purpose and direction to the CAIO. Cyber Florida recommends that the Governance Board be made up of members who are as diverse as possible, since sources of innovations in AI are not restricted to computing fields alone, but instead have spanned psychology, neuroscience, biology, physics, mathematics, cybersecurity and much more. Having a trans-disciplinary governance body will further decisions that are rooted in sound science, ethics and practicality.

Advancing Responsible AI Innovation: The current draft from NIST is comprehensive and presents a detailed list of activities to fuel responsible innovations in AI. We particularly support the clear documentation of AI use cases and periodically re-freshing these as and when AI technologies and intended applications change. We also support the creation of robust cybersecurity policies to better address the needs of AI applications and authorizations to further AI use. The presence of a qualified cybersecurity expert in the AI Governance Body is critical to accomplishing this important goal. Two critical recommendations we make are as follows:

- **Data Storage:** We recommend due diligence in safeguarding data that was trained, validated and tested while developing the AI model. We recommend state of the art access and data control policies in terms of data access and its modifications. With reinforcement learning and federated learning proving to be effective for myriad AI applications, access to current data will be a constant theme, and thereby are increasing avenues for its compromise. Critical recommendations we make are a) the need to store all data within the geographical boundaries of the US; b) multi-layered and fine-grained access control so that impacts of any information leakage are gradual and not catastrophic; c) having a cybersecurity specific Incident Response Plan (adapted to current NIST standards) for AI-centric data and models; and d) investments in homomorphic encryption technologies that allow for AI models trained and executed on encrypted data to enable privacy-preserving AI learning.

- **Periodic AI Model Auditing:** Cyber Florida recommends a robust national scale program to periodically audit all aspects of the AI models, including fidelity of data, security controls, model performance, computing and storage requirements, use-case inventory, test scenarios (in-lab and in the field) and more. We also recommend that NIST create long-term funded and competitive research programs - potentially overseen by agencies like NIST and possibly NSF - that enable non-profit agencies like universities (in collaboration with governmental and military bodies, when possible) to conduct these audits (serving as red teams). Research outcomes will provide impartial reviews to federal agencies, while also ensuring that the next-generation student talent coming out of our universities are well-aware and trained of threats, attacks and countermeasures to ensure safe, accountable and risk-free AI innovation and use, without bias.

Managing Risks from the use of AI: Cyber Florida believes there are clear risks to public safety and rights due to misuse of AI. There is documented evidence of certain governments using AI techniques (most significantly, computer vision) to surreptitiously perform surveillance on civilians, hence infringing upon their rights. There are also reports wherein emergent techniques like Generative AI and LLM models are being utilized for information censorship, misinformation spreading, and denying rights to free speech. As such, this aspect may be the most critical of all to consider in a free and fair democracy like the US and other like-minded nations and allies. These challenges must be detailed and comprehensively described to various stakeholders in the emerging AI space.

In addition, Cyber Florida has the following comments in the avenue of managing risks from AI usage:

- **Create a Comprehensive AI-Compliance Plan:** Cyber Florida recommends the creation of a detailed AI-compliance plan that governmental agencies must enable prior to widespread adoption of AI. The plan can be guided by NIST and must include all aspects of data collection, storage, algorithmic, data protection, fairness, risk and ethical aspects of the entire AI system, including allowed and dis-allowed use cases.
- **Create a comprehensive Incident Response Plan:** Cyber Florida recommends the creation of a comprehensive Incident Response Plan across agencies in the event of any identified misuse of AI. This plan differs from the AI-compliance plan, as the Incident Response Plan will focus on the aftermath of detected AI misuse. While a general template can be the foundation, we recommend a fine-tuned template per agency that considers the specifics within that agency and respective usage of AI. The Response Plan should be comprehensive, covering every aspect of AI usage including data, storage, data access/security policies, AI models, test-scenarios, AI usage history, stakeholders impacted (including the general public), organization of governance board, audit history and more. Cyber Florida also recommends that NIST take the lead in designing guidelines and specifics for such a plan, very similar to what is being done in the cybersecurity arena. Cyber Florida also recommends free and open sharing of such plans across agencies, to commercial entities across the US and the public for their awareness.
- **Cyber Florida recommends the creation of a national-level AI task force with global outlook:** This task force should be comprised of AI experts across diverse spectrum of federal agencies who will specifically monitor,

document and assess AI innovations and use-case across the globe, especially across countries of concern. Having such an agency will not only prepare the US for potential misuse of foreign-developed AI against US citizens, but also help domestic federal agencies assess risk better, which will further strengthen their existing AI innovations and policies as they continue to adapt.

Final Remarks: To summarize, Cyber Florida is delighted at the role NIST is taking in advancing governance, innovation and risk management for agency use of AI technologies. The effort is critical, and will stimulate significant activity across federal agencies, which will eventually permeate into state and local entities serving the nation. We agree with the vision that "AI only works when it works for all of us.". Cyber Florida is delighted to offer its comments to the draft report, and hope that they fine-tune the carefully thought out, comprehensive and timely vision of NIST to practically enable responsible AI governance and innovation while simultaneously protecting our safety and rights.

Contributing Authors

Dr. Sriram Chellappan
Academic Director of Cybersecurity Research,
Cyber Florida: The Florida Center for Cybersecurity
Professor, Computer Science and Engineering,
University of South Florida

Contact Information

Ernie Ferraresso
eferraresso@cyberflorida.org
813 974 1869
Director
Cyber Florida: The Florida Center for Cybersecurity