



Billing Code: 3610-Y8

NATIONAL SECURITY COMMISSION ON ARTIFICIAL INTELLIGENCE

[Docket No.: 05-2020-01]

Solicitation of Written Comments by the National Security Commission on Artificial Intelligence

AGENCY: National Security Commission on Artificial Intelligence

ACTION: Request for comments.

SUMMARY: The National Security Commission on Artificial Intelligence (the “Commission”) was created by Congress in the John S. McCain National Defense Authorization Act for Fiscal Year 2019 to “consider the methods and means necessary to advance the development of artificial intelligence, machine learning, and associated technologies by the United States to comprehensively address the national security and defense needs of the United States.” In connection with this effort, the Commission seeks to learn more about the general public's views on these topics.

DATES: *Comment Date:* The Commission requests comments on or before September 30, 2020 to be considered by the Commission in the formation of its final report.

ADDRESSES: You may submit comments, identified by Docket No. 05-2020-01, by one of the following methods:

- *Email:* inquiry@nscai.gov. Please include the docket number in the subject line of the message.
- *Mail:* National Security Commission on Artificial Intelligence, Attn: RFI COMMENT—Docket No. 05-2020-01, 2530 Crystal Drive, Box 45, Arlington, VA 22202.

- *Fax:* +1-571-778-5049. Please include the docket number on the cover page of the fax.

Due to the ongoing COVID-19 coronavirus pandemic, email is the Commission's primary method of receiving public comment. All submissions received must include the docket number. If the Commission cannot read your comment due to technical difficulties and cannot contact you for clarification, the Commission may not be able to consider your comment. Late comments will be considered as time permits. Please note, any comments received by the Commission may be published online or included with its reports and/or recommendations. Submitters should be aware that the Commission is subject to the Freedom of Information Act and will transfer official records, including comments received, to the National Archives and Records Administration upon termination of the Commission.

Website:

The most current information about the Commission and its activities and recommendations is available on the Commission's website: <https://www.nscai.gov>.

FOR FURTHER INFORMATION CONTACT:

For general inquiries, submission process questions, or any additional information about this request for comments, please contact Tara Rigler by email at inquiry@nscai.gov or by phone at 703-614-6379.

SUPPLEMENTARY INFORMATION:

Background:

The John S. McCain National Defense Authorization Act for Fiscal Year 2019 (FY19 NDAA), Sec. 1051, Pub. L. 115-232, 132 Stat. 1636, 1962-65 (2018), as amended by the

National Defense Authorization Act for Fiscal Year 2020, Sec. 1735, Pub. L. 116-92 (2019), created the National Security Commission on Artificial Intelligence (the “Commission”) to “consider the methods and means necessary to advance the development of artificial intelligence, machine learning, and associated technologies by the United States to comprehensively address the national security and defense needs of the United States.”

Specifically, in Section 1051 of the FY19 NDAA, Congress directed the Commission to consider:

- A. “The competitiveness of the United States in artificial intelligence, machine learning, and other associated technologies, including matters related to national security, defense, public-private partnerships, and investments.”
- B. “Means and methods for the United States to maintain a technological advantage in artificial intelligence, machine learning, and other associated technologies related to national security and defense.”
- C. “Developments and trends in international cooperation and competitiveness, including foreign investments in artificial intelligence, related machine learning, and computer science fields that are materially related to national security and defense.”
- D. “Means by which to foster greater emphasis and investments in basic and advanced research to stimulate private, public, academic and combined initiatives in artificial intelligence, machine learning, and other associated

technologies, to the extent that such efforts have application materially related to national security and defense.”

- E. “Workforce and education incentives to attract and recruit leading talent in artificial intelligence and machine learning disciplines, including science, technology, engineering, and math programs.”
- F. “Risks associated with United States and foreign country advances in military employment of artificial intelligence and machine learning, including international law of armed conflict, international humanitarian law, and escalation dynamics.”
- G. “Associated ethical considerations related to artificial intelligence and machine learning as it will be used for future applications related to national security and defense.”
- H. “Means to establish data standards, and incentivize the sharing of open training data within related national security and defense data-driven industries.”
- I. “Consideration of the evolution of artificial intelligence and appropriate mechanism for managing such technology related to national security and defense.”
- J. “Any other matters the Commission deems relevant to the common defense of the Nation.”

The Commission is required to provide the President and the Congress a final report containing its findings and recommendations regarding these matters no later than March

2021. In connection with this effort, the Commission seeks to learn more about the general public's views on these topics.

Specific Topics to Address:

The Commission invites written comments on any of the topics set forth above under “Background” for which Congress has requested Commission input.

In addition, the Commission would welcome comments on any of the following seven consensus principles from its November 2019 Interim Report, which can be accessed at <https://www.nscai.gov/reports>:

1. Global leadership in AI technology is a matter of national security.
2. Adopting AI for defense and security is an urgent priority.
3. Private sector and government share responsibility for our nation’s future.
4. People matter more than ever in an AI competition.
5. Protecting our most valuable assets and ideas must not come at the expense of free inquiry and innovation.
6. Ethical and trustworthy AI is a strategic and operational necessity.
7. Any use of AI by the United States must have American values—including the rule of law— at its core.

Furthermore, the Commission also welcomes comments related to any of the Commission’s November 2019 Interim Report judgments stemming from the Commission’s lines of effort:

Line of Effort 1 – Invest in AI Research & Development and Software

1. Federal R&D funding for AI has not kept pace with the revolutionary potential it holds or with aggressive investments by competitors.
Investments that are multiple times greater than current levels are needed.
2. Untapped opportunities exist to build a nationwide AI R&D infrastructure and encourage regional innovation “clusters.” Such AI districts for defense would benefit both national security and economic competitiveness.
3. The U.S. government should implement more flexible funding mechanisms to support AI research. Business as usual is insufficient.
4. The U.S. government must identify, prioritize, coordinate, and urgently implement national security-focused AI R&D investments.
5. Bureaucratic and resource constraints are hindering government-affiliated labs and research centers from reaching their full potential in AI R&D.

Line of Effort 2 – Apply AI to National Security Missions

6. AI can help the U.S. Government execute core national security missions, if we let it.
7. Implementation of the government’s national security strategies for AI is threatened by bureaucratic impediments and inertia. Defense and intelligence agencies must urgently accelerate their efforts.
8. Pockets of successful bottom-up innovation exist across the Department of Defense (DoD) and the United States Intelligence Community (IC). These isolated programs cannot translate into strategic change without top-down leadership to overcome organizational barriers.
9. AI adoption and deployment requires a different approach to acquisition.

10. Rapidly fielding AI is an operational necessity. To get there requires investment in resilient, robust, reliable, and secure AI systems.
11. AI is only as good as the infrastructure behind it. Within DoD in particular this infrastructure is severely underdeveloped.
12. The U.S. government is not adequately leveraging basic, commercial AI to improve business practices and save taxpayer dollars. Departments and agencies must modernize to become more effective and cost-efficient.

Line of Effort 3 – Train and Recruit AI Talent

13. National security agencies need to rethink the requirements for an AI-ready workforce. That includes extending familiarity with a range of relevant AI technologies throughout organizations, infusing training on the ethical and responsible development and fielding of AI at every level, and spreading the use of modern software tools.
14. DoD and the IC are failing to capitalize on existing technical talent because they do not have effective ways to identify AI-relevant skills already present in their workforce. They should systematically measure and incentivize the development of those skills.
15. The U.S. Government is not fully utilizing civilian hiring authorities to recruit AI talent. Agencies need to make better use of pipelines for people with STEM training.
16. Expanding AI-focused fellowships and exchange opportunities can give officials and service members access to cutting-edge technology, and bring talent from our top AI companies into federal service.

17. The military and national security agencies are struggling to compete for top AI talent. They need a better pitch, incentive structure, and better on-ramps for recent graduates.
18. American colleges and universities cannot meet the demand for undergraduate student interest in AI and computer science generally.
19. The American AI talent pool depends heavily on international students and workers. Our global competitiveness hinges on our ability to attract and retain top minds from around the world

Line of Effort 4 – Protect and Build Upon U.S. Technological Advantages & Hardware

20. The U.S. Government should continue to use export controls—including multilateral controls—to protect specific U.S. and allied AI hardware advantages, in particular those in semiconductor manufacturing equipment.
21. However, traditional item-based export controls and narrowly-scoped foreign investment reviews are by themselves insufficient to sustain U.S. competitiveness in AI.
22. The United States must continue leading in AI-related hardware, and ensure the government has trusted access to the latest technologies.
23. Law enforcement and academic leaders can and should find common ground on preserving an open research system while reducing security risks from foreign government-directed activity on American campuses.

Line of Effort 5 – Marshal Global AI Cooperation

24. The United States must enhance its competitiveness in AI by establishing a network of partners dedicated to AI data sharing, R&D coordination, capacity building, and talent exchanges.
25. AI presents significant challenges for military interoperability. If the United States and its allies do not coordinate early and often on AI-enabled capabilities, the effectiveness of our military coalitions will suffer.
26. U.S. diplomacy should be open to possible cooperation with China and Russia on promoting AI safety and managing AI's impact on strategic stability.
27. The United States should lead in establishing a positive agenda for cooperation with all nations on AI advances that promise to benefit humanity.

Line of Effort 6 – Ethics and Responsible AI (this cross-cutting priority has been elevated to an identified level of effort since the publication of the November 2019 Interim Report)

28. Developing trustworthy AI systems is essential for operational integrity and adoption. It is closely connected to, and depends on, reliability, robustness, auditability, explainability, and fairness.
29. From the earliest phase, systems should be designed with ethics in mind.
30. Each agency's design and deployment of AI, as with other technologies, must align with America's democratic values and institutional values.
31. Throughout their life cycles, ethical AI systems for national security will need to preserve individual rights and liberties as protected by law. In

international contexts, this includes America's commitments to international humanitarian law and human rights.

Dated: May 22, 2020.

Michael Gable,

Chief of Staff.

[FR Doc. 2020-11453 Filed: 5/27/2020 8:45 am; Publication Date: 5/28/2020]