



RESEARCH
AND ENGINEERING

UNDER SECRETARY OF DEFENSE

3030 DEFENSE PENTAGON
WASHINGTON, DC 20301-3000

CLEARED
For Open Publication

Oct 13, 2023

Department of Defense
OFFICE OF PREPUBLICATION AND SECURITY REVIEW

4 OCT 2023

MEMORANDUM FOR CHAIR, DEFENSE SCIENCE BOARD

SUBJECT: Terms of Reference – Defense Science Board Task Force on Balancing Security, Reliability, and Technological Advantage in Generative Artificial Intelligence for Defense

Interest in traditional Artificial Intelligence (AI) over the last decade has led to advancements in technology and operational efficiencies. As with any maturing technology, this development has split into multiple branches of development, one of which is Generative Artificial Intelligence (GAI). Generative AI is a type of machine learning that takes text prompts as input and produces text, images, or other objects as outputs. The Department of Defense (DoD) will need to leverage ongoing GAI advances in the private sector, develop its own GAI capabilities, and counter GAI capabilities of its adversaries.

As the DoD looks to understand, utilize, and incorporate GAI for both offensive and defensive use, a comprehensive strategy is required to ensure that the Department is a leader in applying this technology. The DoD must also develop options for securing GAI on the battlefield and should continue to develop, alongside U.S. allies and partners, ethical and responsible strategies, and pathways as a means to protect against GAI causing harm.

I am establishing the Task Force on Balancing Security, Reliability, and Technological Advantage in Generative Artificial Intelligence for Defense (“the Task Force”) as a subcommittee of the Defense Science Board (DSB). The DSB, working through the Task Force, should review the state of GAI utilization and integration within the Department and provide recommendations to improve our capabilities, capacity, and resilience and diminish our vulnerabilities and susceptibility to adversary actions. The Task Force should consider, at a minimum:

- Current and future AI technologies suitable for military applications (to include warfighting, defense, test, and evaluation), and steps DoD must take to integrate these technologies. How can DoD better track GAI capabilities that are being developed in the private sector for art-of-the possible application to DoD systems?
- Vulnerabilities in employing GAI capabilities from warfighting, reliability, and security perspectives.
- Measures for ensuring security of GAI applications *and* how to ensure that GAI does not cause unintended harm.
- Application(s) to improve the speed of development and fielding of technologies and capabilities being developed.

- Application(s) to improve the efficiency of analysis, decision making, and operations within USD(R&E).

The Task Force findings, observations and recommendations will be presented to the full DSB for its thorough, open discussion and deliberation at a properly noticed and public meeting, unless it must be closed pursuant to one or more of the exemptions found in subsection 552b(c) of title 5, U.S. Code. The DSB will provide its findings and recommendations to USD(R&E) as the Sponsor of the DSB. The nominal start date of the study period will be within 30 days of the initial appointment of Task Force members. In no event will the duration of the Task Force exceed 12 months from the start date.

In support of this Terms of Reference (ToR) and the work conducted in response to it, the DSB and the Task Force have my full support to meet with Department leaders. The DSB staff, on behalf of the DSB and the Task Force, may request the Office of the Secretary of Defense and DoD Component Heads to timely furnish any requested information, assistance, or access to personnel to the DSB or the Task Force. All requests shall be consistent with applicable laws; applicable security classifications; DoD Instruction 5105.04, "Department of Defense Federal Advisory Committee Management Program"; and this ToR. As special government employee members of a DoD federal advisory committee, the DSB and the Task Force members will not be given any access to DoD networks, to include DoD email systems.

Once material is provided to the DSB and the Task Force, it becomes a permanent part of the DSB's records. All data/information provided is subject to public inspection unless the originating Component office properly marks the data/information with the appropriate classification and Freedom of Information Act exemption categories before the data/information is released to the DSB and the Task Force. The DSB has physical storage capability and electronic storage and communications capability on both unclassified and classified networks to support receipt of material up to the TS/SCI level.

The DSB and the Task Force will operate in conformity with and pursuant to the DSB's charter, chapter 10 of title 5, U.S.; Code, subsection 552b(c); and other applicable federal statutes, regulations, and policy. Individual DSB and Task Force members and the Task Force as a whole do not have the authority to make decisions or provide recommendations on behalf of the DSB nor report directly to any Federal representative. The members of the Task Force and the DSB are subject to certain Federal ethics laws, including section 208 of title 18, U.S. Code, governing conflicts of interest, and the Standards of Ethical Conduct regulations in 5 Code of Federal Regulations, Part 2635.



Heidi Shyu