

AI GUARDRAILS ACT

The Department of Defense must embrace the development and fielding of AI at speed and at scale to maintain its status as the most powerful military force in the world. The U.S. Armed Forces should accelerate efforts to integrate verified and validated AI systems into its military operations, planning, capabilities, training, and doctrine. This is consistent with the Administration's latest AI Action Plan, which notes that "the United States must aggressively adopt AI within its Armed Forces if it is to maintain its global military preeminence while also ensuring, as outlined throughout this Action Plan, that its use of AI is secure and reliable." U.S. law and policy must not just keep up with the pace of technological change but anticipate future trends and applications of AI. Congress must establish left and right parameters around the use of AI in high-stakes scenarios with significant public impact. These safeguards should govern the development, testing, fielding, and continuous post-deployment monitoring of AI in the digital and physical worlds to ensure that the use of AI is safe, secure, and assured.

Militaries must also lay out which decisions must remain under human control regardless of the merits of AI-enabled decision-making. Some military command decisions are too risky and too consequential for machines to decide.

As such, the *AI Guardrails Act* prohibits the use of AI in three DoD use cases:

1. **The launch or detonation of nuclear weapons.** Nuclear weapons are strategic capabilities that have the potential for mass destruction. As such, the decision to launch nuclear weapons should remain solely with the Commander in Chief, not machines.
2. **Domestic mass surveillance.** Our nations laws, including the First, Fourth, and Fourteenth Amendments to the US Constitution, the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq. and the National Security Act of 1947 (50 U.S.C. 3001 et seq.), ensure that people are free from: governmental profiling, targeting, tracking or monitoring based solely on the exercise of freedom of expression, association, or assembly; unreasonable search and seizures by the Government; and discrimination based on, among other things, ethnicity, race, sex, disability, or religion. This provision reinforces these existing protections against government invasion of individuals' privacy and constitutional rights by clearly and explicitly prohibiting the use of DoD AI for domestic mass surveillance.
3. **Autonomous lethal weapon systems without human involvement.** Human accountability is at the core of military command and control. The level of responsibility at which decision authorities are set dictate who is accountable for orders authorizing the use of lethal force. Humans must retain accountability for decisions around the use of lethal force. This provision ensures humans are the ones dictating the left and right parameters of the use of lethal force with AI and autonomous weapon systems.