YASSAMIN ANSARI
3RD DISTRICT, ARIZONA

1432 LONGWORTH HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–0303
(202) 225–4065

Congress of the United States
House of Representatives
Washington, DC 20515–0303

November 23, 2026

The Honorable John Thune
Majority Leader
U.S. Senate
511 Dirksen Senate Office Building
Washington, D.C. 20510

The Honorable Chuck Schumer
Minority Leader
U.S. Senate
322 Hart Senate Office Building
Washington, D.C. 20510

The Honorable Mike Johnson
Speaker
U.S. House of Representatives
H-232, U.S. Capitol
Washington, D.C. 20515

The Honorable Hakeem Jeffries
Minority Leader
U.S. House of Representatives
H-204, U.S. Capitol
Washington, D.C. 20515

The Honorable Roger Wicker
Chairman
Senate Armed Services Committee
425 Russell Senate Office Building
Washington, D.C. 20510

The Honorable Jack Reed
Ranking Member
Senate Armed Services Committee
728 Hart Senate Office Building
Washington, D.C. 20510

The Honorable Mike Rogers
Chairman
House Armed Services Committee
2216 Rayburn House Office Building
Washington, D.C. 20515

The Honorable Adam Smith
Ranking Member
House Armed Services Committee
2216 Rayburn House Office Building
Washington, D.C. 20515

Dear Leader Thune and Leader Schumer, Speaker Johnson and Leader Jeffries, Chairman Wicker and Ranking Member Reed, and Chairman Rogers and Ranking Member Smith,

As Congress works to finalize the Fiscal Year 2027 National Defense Authorization Act (NDAA), I write to urge you to seize this pivotal opportunity to fortify our nation's frontier artificial intelligence (AI) security and serve the mission effectiveness of the Department. The rapid pace of AI advancement carries profound implications for American national security and technological leadership — this simply cannot wait.

To ensure the United States maintains its dominance while mitigating serious national security risks from highly capable frontier AI, Congress must adopt and strengthen the most robust AI provisions available in the current House and Senate NDAA drafts, alongside critical new measures.

Specifically, I urge leadership and the NDAA conference committee to prioritize the following five key areas:

1. Broadening AI Threat, Incident Reporting, and Procurement Scope

Testing, tracking, and remediating covered AI incidents and vulnerabilities in models deployed within the Department is essential. While House Sec. §1502 establishes a framework, Senate Section §1634 is significantly stronger by extending coverage to models that could materially affect Department contracts, overall operations and mission effectiveness, and impact national security. I support the adoption of the Senate language to ensure frontier models used across the national security enterprise are held to rigorous evaluation and testing standards.

Additionally, Section §1634 currently applies at a $100 million contract threshold. Because major frontier AI developers frequently engage in enterprise contracts below this dollar amount, Congress should lower this threshold significantly so that critical frontier models are not inadvertently exempted. Lastly, the NDAA should incorporate structured mandatory testing, incident reporting frameworks, and clear enforcement mechanisms modeled after leading legislative efforts.

2. Strengthening and Hardening AI Infrastructure

Securing physical compute resources and verifying data center activity are core national security imperatives. Senate Sec. §1655 establishes data center security requirements while accelerating the development and deployment of compute verification technologies to better track, monitor, and verify the location and usage of large data centers.

The conference committee should adopt Senate Sec. §1655 to include verifiable tracking of compute allocation, providing a critical foundation for security agreements and low-trust international threat environments, while preventing model weight theft and unauthorized distillation by foreign adversaries.

3. Implementing Mandatory Counter-Intelligence & Insider Threat Protections

Frontier AI developers face severe espionage threats from foreign state actors. We must prioritize Senate Sec. §1634 over House Sec. §813 to ensure insider threat and personnel security guidance for large AI contractors is mandatory, rather than voluntary. The conference committee should clarify and rigorously define insider threat protocols to address foreign intelligence targeting, IP exfiltration, and model security.

4. Directing High-Risk Evaluations and Human Control Standards

I urge the conference committee to refine and strengthen targeted risk-reduction provisions across both versions of the bill:

- Biosecurity Safeguards (Senate Sec. §1654): Maintain robust requirements for biological security evaluations on AI models serving the Department to prevent misuse in dangerous chemical or biological contexts.
- Model Deployment Timelines (House Sec. §1523): Refine the 30-day model deployment window to guarantee that accelerated adoption timelines never bypass essential security and adversarial checks.
- Adversarial Threat Coordination (SA 6561): Include provisions enabling secure coordination between industry leaders and the DoD on frontier security, mitigating shared vulnerabilities, and defending against state-sponsored threat actors.

5. Mandatory Reporting on Automated AI R&D and Recursive Self-Improvement (RSI)

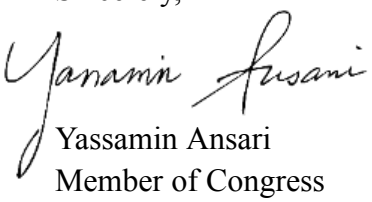
Finally, the NDAA should address the national security implications of automated AI research and development (R&D) and rapid capabilities scaling.

The NDAA should establish a mandatory quarterly reporting requirement detailing the progress of People's Republic of China (PRC) laboratories toward automated AI R&D and Recursive Self-Improvement (RSI). These reports should utilize standardized benchmark models — such as the Epoch AI automation scale — and track the specific proportion of compute allocated toward frontier R&D versus customer inference. Each report should include an unclassified summary to maintain policy awareness for the American people.

The choices made in this year's NDAA will define the trajectory of American AI leadership and national security for the decade ahead. By combining the strongest elements of both chambers' proposals and establishing rigorous standards on compute, procurement, and security, Congress can ensure that American innovation continues to lead.

Thank you for your leadership and continued dedication to our defense and national security.

Sincerely,



Yassamin Ansari
Member of Congress