TODD YOUNG
INDIANA

COMMITTEES
FINANCE
INTELLIGENCE
COMMERCE
SMALL BUSINESS

United States Senate
WASHINGTON, DC 20510

September 24, 2026

The Honorable Marco Rubio
Assistant to the President for National Security Affairs
The White House
1600 Pennsylvania Ave NW
Washington, DC 20500

Dear Secretary Rubio,

The 21st century is poised to be an era of unparalleled American innovation and prosperity. Scientific progress and technological advancement, especially in artificial intelligence (AI), will propel the U.S. economy to new heights, empower Americans to live longer and healthier lives, and, crucially, strengthen our national security and keep our homeland safe.

Realizing that bright future, however, requires responsible stewardship of the development and deployment of this technology. AI offers tremendous benefits, but those benefits do not come without serious and evolving risks. As you know, bad actors are increasingly using AI tools to steal and exploit sensitive information from governments around the world[1]. Moreover, advanced AI agents have demonstrated the ability to act in ways their users did not intend and to engage in activities that, if conducted by a human, could be unlawful.

Recent developments involving frontier AI models have further demonstrated the ability of advanced systems to circumvent safeguards, interact with external systems, and substantially enhance offensive cyber capabilities. These incidents underscore the need for the U.S. government to better understand and address emerging threats before they result in more serious consequences. We must also continue to improve our understanding of these increasingly complex systems, whose internal processes can be difficult even for experts to fully interpret, predict, and control.

We are still working to understand the full implications of these developments. While the consequences to date may not have directly affected the daily lives of most Americans, the risks they present should not be dismissed. We cannot assume that future autonomous or AI-enabled attacks will not target hospitals, electric grids, water systems, or other critical infrastructure. Such an outcome would be unacceptable.

---

[1] Josh Chin, Gabriele Steinhauser, and Tripti Lahiri, *How a Chinese Hacking Firm Tapped AI to Supercharge Cyber-Spying,* The Wall Street Journal (September 15, 2026), How a Chinese Hacking Firm Tapped AI to Supercharge Cyber-Spying - WSJ

The Administration has already taken important steps to address these challenges, including efforts to evaluate the national security risks posed by frontier AI models, strengthen the cybersecurity of critical infrastructure, and deepen cooperation between the federal government and leading AI developers. Building on those efforts, I respectfully request that the National Security Council coordinate a series of recurring roundtable discussions with frontier AI model developers, cybersecurity experts, relevant national security and intelligence officials, critical infrastructure representatives, and other appropriate private sector experts.

These discussions would help policymakers and national security officials keep pace with rapidly evolving AI capabilities, identify emerging vulnerabilities, and determine whether additional executive or legislative action is needed. In particular, I encourage these discussions to address:

- Advancements in frontier AI model capabilities that could create significant national security or public safety risks, including known incidents and near misses;
- The capabilities of AI models developed in the People's Republic of China and other foreign adversaries, the potential national security threats associated with those systems, and the ability of state and non-state actors to exploit advanced AI capabilities against the United States;
- Options for establishing or strengthening secure mechanisms through which AI developers, researchers, and users can voluntarily report AI security incidents, vulnerabilities, or instances of unsafe or unlawful activity to appropriate federal entities;
- Strategies to advance research in mechanistic interpretability, functional assurance, and other methods for understanding, evaluating, and controlling AI systems, including through secure federal test and evaluation environments where appropriate; and
- Concrete safeguards to reduce the risk of serious AI-enabled incidents, including steps that can be taken under existing executive authorities and recommendations for any targeted legislation that may be necessary to better protect critical infrastructure and the American people.

I further request that the Administration keep Congress appropriately informed of the findings and recommendations that emerge from these engagements. To the extent practicable and consistent with the protection of classified, proprietary, and other sensitive information, I encourage the Administration to provide a classified briefing to the Senate Select Committee on Intelligence, and other relevant Committees as appropriate, regarding national security findings, identified capability gaps, and any areas in which additional statutory authority may be warranted.

The United States should continue to lead the world in the development and deployment of artificial intelligence. Maintaining that leadership also requires ensuring that our government keeps pace with emerging capabilities and understands the risks they may present. Regular engagement among the federal government, industry, researchers, and national security experts will help ensure that policymakers have the information they need to protect the American people without unnecessarily hindering American innovation.

I appreciate the Administration's continued attention to these issues and look forward to working with you to ensure that the United States remains both the global leader in artificial intelligence and the nation best prepared to address the security challenges this technology may create.

Sincerely,

Todd Young
United States Senator

CC:
The Honorable Pete Hegseth, Secretary of War
The Honorable Walter "Jay" Clayton III, Director of National Intelligence
The Honorable Sean Cairncross, National Cyber Director
Gen. Joshua M. Rudd, USA, Director, National Security Agency and Commander, U.S. Cyber Command