Jason Matheny Statement to the House Permanent Select Committee on Intelligence

Chairman Turner, Ranking Member Himes, members of the committee: Good morning, and thank you for the opportunity to talk with you today. I'm the President and CEO of the RAND Corporation, a nonprofit and nonpartisan research organization. Before RAND, I served in the White House National Security Council and Office of Science and Technology Policy; I served as a Commissioner on the National Security Commission on Artificial Intelligence, to which I was appointed by the Senate Select Committee on Intelligence; and I served as Assistant Director of National Intelligence and as Director of the Intelligence Advanced Research Projects Activity, which develops advanced technologies for the U.S. intelligence community.

Our nation faces many significant national security challenges. Among them are an increasingly belligerent Russia, an intensifying competition with China that features not just military rivalry but also competition in key economic and technological domains, and continued provocations by North Korea and Iran. RAND has for decades helped decisionmakers confront these issues, and today we are ramping up our research significantly in key areas—including in understanding China, its economy, and its leadership's intentions—while we're building new analytic tools for supporting U.S. economic and technology strategies.

But today, I want to focus on two significant threats to national security deserving greater focus and attention: advances in synthetic biology, or *synbio*, and artificial intelligence, or *AI*. These two technologies stand out for both their rates of progress and the scope of their applications. Both hold the potential to broadly transform entire industries, including ones critical to the United States' future economic competitiveness, such as medicine, manufacturing, and energy. Synbio and AI also pose grave security challenges for which we are currently unprepared. In the case of synbio, new tools could enable a state, group, or individual to construct novel viruses capable of killing many millions of people, whether intentionally or unintentionally. In the case of AI, new tools could be used to create novel cyber weapons and disinformation attacks at an unprecedented scale.

Synbio and AI create significant challenges for national intelligence. For example,

- The technologies are often driven by commercial entities that are frequently outside of U.S. intelligence collection priorities.
- The technologies are advancing quickly, typically outpacing policies and organizational reforms within government.
- Assessments of the technologies require expertise that is concentrated in the private sector and that has rarely been involved in national security.
- The technologies lack conventional intelligence signatures that distinguish benign from malicious use or that distinguish intentional from accidental misuse.

Addressing these risks may require some structural reforms in the intelligence community, and I will highlight six specific actions the IC could take:

1. Ensure an increased national intelligence emphasis on emerging and disruptive technology topics, especially synbio and AI, including through the National Intelligence Priorities Framework, Key Intelligence Questions, and Collection Emphasis Memos.
2. Require a scientific and technological intelligence strategy to significantly expand collection and analysis of information on key foreign public- and private-sector actors in authoritarian states involved in synbio and AI. The strategy could be informed by a survey on the value of, accessibility to, and unmet need for S&T intelligence, particularly among federal S&T organizations; the Departments of Commerce, Treasury, and State; and key U.S. allies.
3. Strengthen the IC's institutional capacity for carrying out such a strategy (1) by creating new partnerships and information-sharing agreements among government agencies, academic labs, and industrial firms and (2) by identifying hundreds of the private sector's leading scientists, engineers, and technologists, who can obtain security clearances to advise the government on key technology developments.
4. Strengthen the IC's capacity to lead National Intelligence Estimates and Net Assessments on global trends in synbio and AI that include assessments of key foreign public and private entities; their infrastructure, investments, and capabilities; their supply chains of tools, material, and talent; and the risks of intentional or accidental misuse of their technologies. Accurate assessments will rely on drawing in cleared experts from the private sector.
5. Encourage the creation of an IC framework to share classified S&T intelligence with allied high-technology nations, such as the Five Eyes countries, plus France, Germany, Japan, the Netherlands, Singapore, and South Korea.
6. Encourage the development of a communications strategy to disclose authoritarian countries' violations of technology-related norms and treaties that affect public safety, human rights, and global security. The strategy could outline an equities process for prioritizing the declassification of intelligence that can be used in public diplomacy, as well as opportunities to better leverage unclassified sources.

I thank the committee for the opportunity to speak with you today, and I look forward to your questions.