COMMITTEE ON HOMELAND SECURITY
Ranking Member Bennie G. Thompson

FOR IMMEDIATE RELEASE

Hearing Statement of Counterterrorism, Law Enforcement & Intelligence Subcommittee Ranking Member Seth Magaziner (D-RI)

A Security Sprint: Assessing the U.S. Homeland's Vulnerabilities to Chinese Communist Party Aggression

May 23, 2023

It is indisputable that the Chinese Communist Party is the United States' greatest competitor on the world stage. And it is indisputable that the CCP is actively trying to undermine the economy and security of the United States at home and abroad. As I reiterated in our last hearing on this topic in March, the threat emanating from China is from the CCP as they have become more aggressive in trying to undermine U.S. interests, not the Chinese people.

At the outset, I think it is important to highlight that this competition we find ourselves in touches upon many areas, from defense to foreign policy to political ideology, but is first and foremost an economic competition. That is why the CCP has aggressively pursued unfair economic practices like currency devaluation, the use of weak and inhumane labor standards, and in particular intellectual property theft, targeting both United States government agencies and U.S. companies in its effort to usurp our global economic leadership.

The CCP routinely uses espionage and cyber exploitation to steal American intellectual property, trade secrets, and even defense information. Each year, China's economic espionage against American businesses costs between $225 and $600 billion, according to the FBI. In 2020, just one Chinese national stole intellectual property worth a billion dollars from his employer, a U.S. petroleum company.

Just. One. Person.

And last year, a Boston-based cybersecurity firm, Cyberreason, found that a Chinese state actor had exfiltrated hundreds of gigabytes of IP and sensitive data from about 30 companies around the world. The estimated cost of that IP loss runs into the trillions.

But even more alarming is that the intellectual property stolen by China did not just include commercial product designs and trademarks for cheap, knock-off counterfeit trinkets – it included blueprints for fighter jets, helicopters, missiles, pharmaceuticals, and large-scale technologies. These thefts of intellectual property and trade secrets threaten our national defense, and also reduces the economic advantage of the United States, hurting our companies and costing American jobs, — and the CCP does not plan to stop.

The CCP has plans to become more assertive. Its "Made in China 2025," or MIC2025, initiative lays out a broad set of industrial plans that aim to boost China's competitiveness by advancing its position in manufacturing and supply chains. Over the past decade, the CCP has also used foreign investments through its Belt and Road Initiative to develop China-centered and -controlled global infrastructure, transportation, trade, and production networks. This unprecedented initiative is more than just an

economic challenge to the United States – it is expanding China's reach into hundreds of countries around the world and reducing the costs of doing business with China.

Perhaps most troublingly, Belt and Road investments in building next-generation digital networks worldwide are giving the Chinese Communist Party access to troves of sensitive data from around the world, which it can use against the United States. How does the CCP plan to advance its position? By using every tool at its disposal—including spycraft—to leapfrog into emerging technologies. U.S. officials and cybersecurity analysts have described MIC2025 as a blueprint for the types of companies and industries China will target through espionage and hacking. FBI Director Christopher Wray put the CCP threat into perspective when he said, quote, "[t]he greatest long-term threat to our nation's information and intellectual property, and to our economic vitality, is the counterintelligence and economic espionage threat from China."

I am pleased that under the leadership of President Biden and Secretary Mayorkas, DHS finally issued the Quadrennial Homeland Security Review — the first in nine years. The 2023 review directly tackles the threat posed by the Chinese Communist Party to our competitiveness, democratic institutions, and homeland security. I am pleased that the Biden Administration has taken the threat of the CCP seriously with the passage of the Chips and Science Act, the establishment of the China House at the State Department, and the 90 Day Sprint at DHS.

I look forward to hearing from today's witnesses about the broad threats the United States faces because of the Chinese Communist Party. I am particularly interested in hearing how DHS and the FBI work with Federal partners to protect American businesses and the government from CCP espionage. Furthermore, I look forward to hearing how DHS is implementing the Biden Administration's Quadrennial Homeland Security Review and receiving an update on the status of the DHS 90-day sprint on China.

# # #

Media contact: Adam Comis at 202-225-9978