

Chairman Mark R. Warner Opening Statement

Protecting American Innovation: Industry, Academia, and the National Counterintelligence and Security Center

U.S. Senate Select Committee on Intelligence Open Hearing September 21, 2022

Good afternoon; I call this Hearing to order. Welcome to our non-government expert witnesses:

- **The Honorable Bill Evanina**, former Director of the National Counterintelligence and Security Center. He is the founder and CEO of the Evanina Group;
- **The Honorable Michelle Van Cleave**, Senior Advisor, Jack Kemp Foundation and Former National Counterintelligence Executive, at the Office of the Director of National Intelligence;
- **Dr. Kevin Gamache**, Vice Chancellor and Chief Research Officer, at the Texas A&M University System; and
- **Mr. Robert Sheldon**, Director, Public Policy & Strategy, at CrowdStrike

Today's hearing, "Protecting American Innovation: Industry, Academia, and the National Counterintelligence and Security Center," will examine the implications of the findings of our Committee's bipartisan report on the National Counterintelligence and Security Center (or NCSC), which we publicly released yesterday.

This is the first in a series of hearings on the report, and future hearings will include current U.S. counterintelligence officials to discuss in more depth concrete changes that may be necessary for the NCSC and the government's counterintelligence enterprise.

Our nation faces a dramatically different threat landscape than it did even a couple of decades ago. Today's foreign intelligence threats are not just targeting the government, but are increasingly looking at the private sector to gain a technological edge over our key industries. As much as \$600 billion worth of US intellectual property is stolen each year. New threats and emerging technologies mean that we need to make serious and substantive adjustments to how we address the issue of counterintelligence if we are to protect America's national and economic security.

For many years the Members of this Committee were constantly hearing the “alarm bell ringing” when we got briefings on these foreign intelligence threats, but we felt it important not just to be made *aware* of the threat, but also to *do something* about it. So the Committee – in a bipartisan way, thanks in part to Senators Rubio, Burr, Cornyn and Collins – convened a series of classified sessions with the Intelligence Community and leaders from the private sector, tech companies and academia... to brief them on efforts by the Communist Party of China to target key U.S. technologies for acquisition and development.

These include aerospace... advanced manufacturing... artificial intelligence... biotech... data analytics... new materials... semiconductors, and renewables... in order to ensure PRC’s future dominance in these areas. We saw the CCP’s approach with their pursuit of 5G supremacy, and I am proud of the Committee’s bipartisan work in sounding the alarm on the threat that China’s domination of 5G communications technology would pose to U.S. and allied interests.

FBI Director Wray has stated that the Bureau opens up a new PRC-related counterintelligence investigation every 12 hours, and that China has stolen more of Americans’ personal and corporate data than every other nation combined.

With this hearing, we are broadening our counterintelligence focus to also look at the malign role played by other large state adversaries like Russia, as well as other nations such as Iran and North Korea.

As we discuss what the CCP is doing in the United States, I want to make myself crystal clear – my concern lies squarely with Xi Jinping and Chinese Communist Party leaders, not the people of China, and certainly not with Chinese- or Asian-Americans, who have contributed so much to our society. And similarly, recall those brave Russians who came out to the streets to protest Vladimir Putin’s war and the arrest of Alexei Navalny. Our beef is not with the Russian people or immigrants of Russian descent, but with the kleptocratic and murderous regime of Putin.

The Committee’s report is the product of years of independent research by non-partisan Committee staff to assess the mission, authorities and resourcing of the NCSC and its mission to coordinate the government’s counterintelligence efforts. Among the report’s findings are:

- The United States faces threats from a wide variety of adversaries, including powerful state rivals such as China and Russia, regional adversaries, minor states aligned with U.S. adversaries, ideologically motivated entities, and transnational criminal organizations;
- Foreign intelligence entities are targeting a wide set of public and private entities, including U.S. government departments and agencies that are not part of the intelligence community, national laboratories, the financial sector, the U.S. industrial base, and academia;

- Today’s adversaries have access to a much wider variety of tools for stealing information, influencing U.S. officials, or inflaming social and political tensions than in the past, including nontraditional human, cyber, advanced technical, and open source intelligence operations to collect against U.S. plans and policies, sensitive technology, personally identifiable information, and intellectual property, as well as to influence U.S. decision-making and public opinion; and
- Despite the wide-ranging and sophisticated number of counterintelligence threats facing the U.S., the U.S. counterintelligence enterprise is not postured to confront the whole-of-society threat landscape facing the country today, with the NCSC lacking a clear mission as well as sufficient and well-defined authorities and resources to effectively confront this landscape.

The core questions for this hearing are: What role should academia and industry play in protecting information with national security implications? Are any legislative or policy changes needed to codify this role? What government resources may be needed to help academia and industry protect their data, technologies, and people?

What role is NCSC—as the lead agency for national counterintelligence—expected to play in informing, coordinating with, and supporting these entities? And given the increasingly important role of counterintelligence due to these changes in the foreign threat landscape, does the U.S. government need an independent counterintelligence agency to tackle them?

With no consensus on the NCSC’s existing mandate and path forward, Congress, in conjunction with the Executive Branch and the Office of the Director of National Intelligence (ODNI), must develop a consistent U.S. government-wide definition of counterintelligence that reflects today’s threat landscape. We must also enact reforms to clarify NCSC's mission, structure and responsibilities... and determine what, if any, role it should play in traditional, strategic and offensive counterintelligence operations.

Today’s hearing should serve as a catalyst for a long-overdue discussion on concrete steps to reform US counterintelligence in light of today’s foreign adversary threat landscape. Given the stakes, we should not be afraid to consider big, bold changes. I look forward to the witnesses’ testimony.

For Members’ information, we will be asking questions by **order of seniority** – in 5 minute rounds.

Thank you. I now recognize the Vice Chairman.