Office of the Director of National Intelligence

Statement by Robert "Bear" Bryant, National Counterintelligence Executive, upon the release of "The Report to Congress on Foreign Economic Collection and Industrial Espionage"

Ronald Reagan Building & National Trade Center
Washington, D.C.
9:00 a.m.
Thursday, November 3, 2011

ROBERT "BEAR" BRYANT: Good morning. This is impressive – standing room only. Thank you for joining us this morning. I know it's early to be diving into the exciting world of economic espionage and global economies. But I appreciate you being here because I view this as a critical issue. The latest report to Congress on foreign economic collection and industrial espionage is entitled, "Foreign Spies Stealing U.S. Economic Secrets in Cyberspace."

Protecting intellectual property is key to U.S. economic growth. It is obvious to me in the days and past in the 1970s, the primary asset of our corporate America were tangible assets. Today I would say the primary assets of corporate idea are intangible assets – certainly research and development, certainly plans and business plans, and really positions on contracts. The threat to the U.S. private sector is more exposed and vulnerable than ever.

Estimates from academic literature on the losses from economic espionage range so widely in my mind; they go from 2 billion (dollars) to 400 billion (dollars) – they're almost meaningless. All we know is that the losses are extremely significant and they're extremely harmful to our national well-being.

What I can tell you is that our most valuable information are usually of general interest to foreign collectors. Public and private research and development, according to various estimates, the target is $400 billion. That's what our R&D each year is, developed by American corporations. This is the target. And frankly, it's all in a cyber position.

The private sector – we need to work with – together with. It has to – we have to have a better partnership between the federal government, the intelligence community, the private sector and academia to ensure that we're talking to each other, we're sharing information and if there's a threat to really the cyber R&D, we know about it and vice versa, we talk to each other. This is a quiet menace to our economy, with notably big results. Trade secrets developed over thousands of working hours by our brightest minds are stolen in a split second and transferred to our competitors.

In 2006, a Ford engineer copied 4,000 documents to an external hard drive just before he was to start work with a rival company in China. In 2009, a chemist downloaded information about organic light-emitting diodes to his personal email account and thumb drive, intending to transfer this data to Peking University, where a position awaited him.

In 2009, also, a chemist at Valspar Corporation downloaded secret formulas for paints and coatings from the corporation's network to take a new job with a rival in Shanghai. In 2010, there were more prosecutions for economic espionage against the United States by entities and individuals purporting to act on behalf of foreign countries, particularly Russian and China.

The one thing I would say is we at this time are at a critical moment. The theft of research and development from our national economy is a time to have a national discussion. And the purpose of this report is to – is to basically bring this issue out and come up with thoughts and solutions to really protect our research and development and to go forward in a world that is very, very complicated, because we have a global economy.

I would just point out that what I see as economic espionage, to a large extent, is really kind of a death by a thousand cuts. We continually have, what I see almost daily across my desk, where we have incursions on very, very significant information. And these are being perpetrated by different actors – sometimes foreign intelligence services, sometimes by corporations, sometimes by individuals.

I would just say that we have to understand that in 1996 when the economic espionage statute was proposed by the FBI and subsequently passed, that was the year Google became a corporation. And so how much has changed in that time is very significant. I would just like to add that – before I turn this over to the panel and they make their presentation – one thing.

I'd just like to give a word of thanks to my predecessor, Joel Brenner, at NCIX. He was the one, when I came on, that basically raised what I call the clarion call to this issue of economic espionage. And I just wanted to say that for an accolade to this person.