

WELCOMING REMARKS

By Joel F. Brenner

DNI'S PRIVATE SECTOR SYMPOSIUM ON INSIDER THREATS

Carnegie Endowment for International Peace

1779 Massachusetts Avenue, NW

Washington, DC 20036

30 May 2007

Welcome to the fourth in a series of symposia between the Office of the Director of National Intelligence and the private sector. I'm Joel Brenner, the National Counter-intelligence Executive, in the Office of the DNI.

Compared with the budget of, say, 30 years ago, the intelligence community spends vastly increased sums, and a vastly increased percentage of its budget, on contracts with the private sector. The implications of this comparison are enormous. The dramatically more extensive and intensive relationship between intelligence agencies and the private sector affects every important aspect of how we do business: acquisition practices, personnel policies and mobility, privacy and data rules, intellectual property, and of course security.

Three weeks ago, a federal jury in California found Chi Mak, a U.S. citizen of Chinese extraction, guilty of conspiring to violate export control laws and of acting as a foreign agent without registering as such. I won't discuss the evidence in that case in any detail since it's still winding its way through

the courts. It's enough for our purposes this morning to note that the case involved the loss of highly sensitive radar and quiet-drive naval technology that cost *billions* to develop. But what makes *Chi Mak* different from other espionage cases is not the gravity of the loss; unfortunately we've suffered grave losses before. What's different is that Chi Mak was never a government employee. He was employed instead by a company called Power Paragon, Inc., a subsidiary of L3, which, like your companies, is a government contractor. And it is that vulnerability that brings us together today to consider the changing nature of the insider threat and its extension to the private sector.

From a counterintelligence point of view – and counterintelligence is what I get paid to think about – the seismic shift toward increasing reliance on the private sector in the intelligence world means that you in the private sector and we in the intelligence world are now squarely facing many of the same counterintelligence risks.

Broadly speaking, our risk comes in three varieties: (1) risk of old-fashioned espionage, (2) risk from electronic network vulnerability, and (3) risk from acquisition vulnerability, by which I mean the purchasing of hardware and software whose provenance is murky and which may

contain what we call hooks or backdoors to facilitate electronic espionage. The last two sorts of risk are of course related and they are the new frontiers of counterintelligence. If you can exfiltrate massive amounts of information from your office in Shanghai or Moscow through network penetrations, and if you can facilitate those penetrations through backdoors in equipment purchased by U.S. companies or the federal government, you may not have to plant or suborn an insider to cause us grave harm. Yet the insider risk remains a counterintelligence nightmare. Why? Not because it's more important than the other sorts of risk I just mentioned, but because the risk of a treasonous insider, when combined with network and acquisition risks, represents the potential for a perfect storm of a disastrous loss of military secrets, public and private intellectual property, intelligence assets, and governmental and corporate intentions at the highest levels – not to mention economic, financial, and logistical chaos or the degradation of public trust in supposedly trusted networks.

This risk is now your risk in the private sector as well as our risk in government. The equivalence between national security information and government secrets, which in this country was never perfect to begin with, has now eroded

almost completely. To put it another way, when it comes to national security, the boundary between public and private has more or less vanished.

As we note in the new National Counterintelligence Strategy – which the President recently approved and which I commend to your reading – foreign intelligence activities extend beyond traditional targets in the intelligence community and Departments of Defense and State. The private sector and academia are fertile breeding grounds for advanced scientific discovery, cutting-edge technology, and advanced research and development that make them irresistible targets – and in many cases, soft targets – for foreign intelligence services. And technology is often targeted well before its final development. Vital assets are vulnerable during their entire lifecycle – from the research and development states, through acquisition and operational testing, and into manufacturing and deployment. For example, when a U.S. company or university funds cutting-edge research and development, the results may be stolen, taken abroad, and incorporated into foreign products for sale back into the U.S. market. This is happening, and it is happening in a systematic, targeted manner.

The risk to you in the private sector extends well beyond the classified work you do for the government. Foreign intelligence services target you for commercial technology that is unlikely ever to be classified. The counterintelligence problem, therefore, is no longer just a government problem. Counterintelligence is a problem for every firm that has secrets to protect.

For these reasons, we in the intelligence community have committed ourselves to engage the private sector, academia, and the general public in an on-going dialogue regarding the threats we face and the way we should respond to them. I emphasize the word “dialogue.” We have much to learn from each other, and we in government are listening as well as talking.

This morning we’ll be breaking into four working groups on: (1) insider cyber vulnerability, (2) insider criminal activities, (3) insider economic espionage, and (4) insider terrorist activities. (As a former prosecutor and graduate of the London School of Economics who is beating the drum on cyber vulnerabilities, I’m thoroughly conflicted on which group I belong in.) Before we do that, however, I want to introduce Steve Nixon, the Deputy Associate Director of National Intelligence for Science and Technology, and my

old friend Arnaud de Borchgrave, who will each say a few words.