NCIX
NATIONAL COUNTERINTELLIGENCE EXECUTIVE

REMARKS OF JOEL F. BRENNER

NATIONAL COUNTERINTELLIGENCE EXECUTIVE

"Strategic Counterintelligence"

American Bar Association
Standing Committee on Law and National Security
The University Club, Washington DC
8:00 AM, 29 March 2007

Mr. Harvey and members of the Standing Committee, it's a great privilege to speak to you this morning – to address a committee whose meetings I've been attending since 1985 and which, even in the midst of sometimes bitter partisan political wrangling, has remained a bastion of rational discourse among people of different points of view. In a political culture in which the active partisans of civil liberty under law and the active partisans of national security don't overlap quite as often as we might like, this committee

has been a steadfast member of both camps. So am I. By the way, it was through this committee that I moved from commercial lawyering to being the Inspector General of NSA and now the National Counterintelligence Executive. So the committee has played a pivotal role in my professional life, and it is a particular honor and pleasure to be invited to address you.

Counterintelligence: What It Is

When former Director of National Intelligence John Negroponte appointed me as the National Counter-intelligence Executive, lots of people I knew said, "Counterintelligence? Wow, Brenner! Sounds fascinating. But … what is it?" So I'm going to begin by answering that question.

Counterintelligence is the business of identifying and dealing with foreign intelligence threats to the United States. Its core concern is the foreign intelligence services of foreign states and the similar organizations of non-state actors --

transnational terrorist groups such as al Qa'ida and Lebanese Hizbollah, for instance. Counterintelligence has both a defensive mission — protecting the nation's secrets and assets against foreign intelligence penetration — and an offensive mission — finding out what foreign intelligence organizations are up to in order to better defeat their aims. The protective, defensive mission is easier for Americans to relate to, because in our offensive mission we are really trying to do unto others what we do *not* want them to do unto us. We Americans are idealistic, and this line of work is not run according to the golden rule.

Even in an idealistic nation, however, we have been victimized by the treachery of some of our fellow citizens. For example, FBI agent Robert Hanssen spied for the Soviets/Russians for close to two decades and gave them continuity of government information they could have used to defeat us decisively if war had broken out.

The Walker spy ring provided the Soviets with the crypto material that let them read more than a million messages to our ships and submarines at sea.

The Conrad spy ring compromised to the Soviets the war planning for the defense of Europe. The judge at Conrad's trial wrote: "If war had broken out between NATO and the Warsaw Pact, the West would have faced certain defeat."

CIA case officer Aldrich Ames compromised hundreds of CIA, DoD, and FBI human agent operations. Because of what he did, virtually our entire network against the Soviets was *wiped out* — imprisoned or killed.

Espionage did not go away with the end of the Cold War. It is older than Joshua's reconnoitering of the Promised Land, and it will be with us forever. Much of the damage Hanssen did, for example, was done after the collapse of the Soviet Union. And much more recently, DIA analyst Ana Montes was caught after a 15-year campaign of

spying against us for the Cubans, who are very good at this business. Montes compromised our entire program against Cuba — electronic as well as human.

Preventing penetrations like these, and ferreting them out early when we can't prevent them, is part of what counterintelligence agencies do. The job is not getting easier. There are now 140 foreign intelligence services that try to penetrate the United States or U.S. organizations abroad, and for many of them, we are their number one target.

When our adversaries succeed in penetrating us, policymakers, the Congress, and the American people lose confidence in the intelligence we ourselves produce. And when that confidence is lost, regaining it is difficult. Meanwhile our security is at risk, and we bleed technology, both civilian and military.

Right now – this week – the *Chi Mak* case is in trial in the Central District of California. The case broke when the

government arrested Chi Mak's brother and his wife about to board a plane for China carrying encrypted computer disks hidden among innocuous commercial CDs. The encrypted files contained export-controlled documents relating to the U.S. Navy's next generation (DDX) warship. When the FBI executed a search warrant at the defendant's house, they discovered hundreds of classified defense-related documents and tasking lists from the Chinese government to which the documents were responsive. I should add that Chi Mak worked as a contractor on the Navy's quiet electric drive, the technology designed to suppress the signature emitted by our submarines and surface warships. Under questioning, he admitted that he had been passing information to the Chinese since 1983, and that the technologies he had compromised included the power distribution technology for the Aegis cruiser's radar system.

This compromise is not small potatoes. It shortens by years the technological advantage of the U.S. Navy. It

degrades the Navy's deterrent capability in the Taiwan Strait. And it puts the lives of our sons and daughters in the Navy at risk. From a purely fiscal point of view, it also means the Chinese are leveraging the American R&D budget — your tax dollars and mine — in support of their own war-fighting capability.

And that, ladies and gentlemen, is the world we live in and why you should care about our ability to counter this kind of intelligence onslaught.

Now with that background I want to do three things: First, I'm going to describe to you what my job is and is not. Second, I'm going to tell you what I've done in my first six months. Third, I'm going to share with you my views on the major challenges we face going forward.

The NCIX: Who he is and Isn't

First, as to my job: I work for the Director of National Intelligence, Mike McConnell. I say "intelligence" and not "security." Think of it this way: If there's a hole in your

fence, security's job is to fix it. Our job (in part) is to figure out how it got there, who's been coming through it, and what they took with them when they left. We work closely with security, but we're in a different line of work.

By the Counterintelligence Enhancement Act of 2002, Congress has charged me with promulgating a strategy for all counterintelligence elements of the U.S. Government, and to review it annually. And it has charged my office with (1) integrating the activities of all our counterintelligence programs to make them coherent and efficient, (2) coordinating counterintelligence policy and budgets to the same end, and (3) evaluating the performance of the counterintelligence community against the Strategy.

The key noun here is "strategy." The key verbs are "integrate," "coordinate," and "evaluate." My office doesn't do operations. In fact, Congress prohibited me from engaging in operations and was right to do so. It would be strange indeed even to attempt to run operations from an

office whose mission is strategy, policy, and integration. In any event, the business of writing strategy, evaluating its implementation, and coordinating the disparate counterintelligence elements of the federal government is a full-time job, I assure you.

On the other hand, if I am to evaluate the implementation of strategy, I must have sufficient visibility into operations to carry out my responsibilities. I've got to know what and how well we are doing at the job of preventing and either manipulating or rolling up foreign penetrations, and at the job of returning the favor to our adversaries. My predecessors did not have that visibility. Now that the DNI has made me the "mission manager" of counterintelligence, however, and thanks to the cooperation of my colleagues in the agencies, I am gaining it rapidly.

What I've Done in Six Months

Now let's turn to my first six months. In that period I accomplished three things I want to tell you about:

First, I reconvened the National Counterintelligence Policy Board, the primary interagency group that develops policy and coordinates activities. It is composed of representatives of the nine agencies with the largest counterintelligence elements. But when I took over, the Board had not met in about eighteen months. This was unfortunate. If you want a collection of stovepiped agencies to start acting like a joint enterprise, you can't get there by issuing edicts. You've got to make use of the available interagency mechanisms – or invent new ones. That's what the Policy Board does. Frankly, what we're doing is institutional behavior modification, little by little. The Board now meets every month, and it does serious business through interagency working groups devoted to particular problems or issues.

Second, at my urging, the DNI has just recommended to the NSC to move counterintelligence from a lower to a top priority in the National Intelligence Priorities Framework.

There are never enough collection assets to collect against every target of opportunity, so where you stand in the priority list tells you a lot about how important your mission is. If our recommendation is implemented, it's therefore going to make a real difference every single day to counter-intelligence analysis.

Third, I used the Policy Board as the consultative mechanism to develop a new *National Counterintelligence Strategy*. The *Strategy* was approved by the President last week, and its unclassified version became available on-line just two days ago. You can find it on the NCIX website and on the website of this committee. It's different from the old one in three ways. (1) It was the result of an intensive coordination process and therefore represents a real meeting of the minds among different agencies about what we need to do. (2) It is far more specific than the old one. And (3) consequences will flow from it — operational and

budgetary consequences. Strategy must be driven from the clouds down to the sidewalk or it's meaningless.

(Let me digress here a second. We drafted this Strategy and coordinated it through the Under Secretary of Defense for Intelligence, the Departments of Energy, Justice and State, the CIA, the FBI and the Joint Chiefs of Staff in about 75 days — a minor miracle, if I say so myself. I could not have done that without the whole-hearted support of all those organizations. This was coordinated government at its best – and a pretty good initial metric for how we're doing.)

Strategy and New Frontiers

The new Strategy addresses counterintelligence at a strategic level. Strategic counterintelligence (as opposed, say, to running operations) means two things: (1) Bringing coherence to the disparate activities of the CI community, and (2) looking over the horizon to anticipate tomorrow's needs. How will the world look in three or five or ten years? What are the cultures and languages which we will wish we

had begun studying now, in the year 2007, rather than in 2015? We've got to do better at this.

In my judgment, we face two new strategic counterintelligence frontiers: Network vulnerability and acquisition vulnerability. The nation's electronic networks are too easy to hack, and the number of world-class hackers is multiplying at bewildering speed. If you can exfiltrate massive amounts of information electronically from the comfort of your own office on another continent, why incur the expense and risk of running a spy?

We face similar risks when we buy equipment for the intelligence agencies. What does "Made in USA" mean when components come from overseas and the software in the electronics may have been written by God-only-knows-whom? Unknown or sketchy provenance raises the risk that a foreign government or organization could program vulnerabilities into our most sensitive information systems.

The new strategy addresses these problems in more detail than I can do here, so I hope you'll be curious enough to punch it up and read it, and if you have comments about it, I'd be grateful if you'd share them with me.

Intelligence Under Law

I want to leave time for questions, so let me close now with a comment that goes to the heart of this committee's mission, namely, the pursuit of national security missions under law. U.S. counterintelligence organizations may be imperfect but they are very good. We have highly skilled, dedicated professionals all over the world who accomplish difficult tasks every day in often hostile environments. We did not get good by breaking American law. We did it within our laws and Constitution, and we cannot lose sight of the fact that what we are trying to protect is, above all, the rule of democratically made law. America's position in the world is best secured by sustaining her values. We who labor in intelligence work in powerful, secret agencies on behalf of a

society that profoundly distrusts both power and secrecy, and in the long run, we cannot function effectively unless the country we serve believes that we do our work within the law. If the Congress believes it is faced with systematic violations of the law, the tools available to it are limited. It uses a meat ax, not a scalpel. We went through such a period after the investigations of intelligence abuses in the mid-1970s, and those of us in the business don't want it to happen again. Those of us who remember that era – and we are retiring at a rapid rate – therefore have a duty to teach our juniors that intelligence must be conducted in compliance with US law and the United States Constitution, or we are asking for trouble. Ladies and gentlemen, it's time we recognized that intelligence is a regulated industry, and in any regulated industry, *compliance is good business.*

Conclusion

Mr. Harvey and members of the Standing Committee, I'll happily take your questions.

###