Department of Justice

FOR IMMEDIATE RELEASE NSD

MONDAY, DECEMBER 10, 2007 (202) 514-2007

WWW.USDOJ.GOV TDD (202) 514-1888

PREPARED REMARKS OF KENNETH L. WAINSTEIN

ASSISTANT ATTORNEY GENERAL FOR NATIONAL SECURITY AT THE

PRACTISING LAW INSTITUTE'S 2007 EXPORT CONTROL CONFERENCE

WASHINGTON, D.C.

Good morning everyone. I want to thank the Practising Law Institute for inviting me to participate in this conference. I'm pleased to be here and to have this opportunity to discuss the important topic of export control enforcement with all of you.

I. The Threat

At this conference, you'll hear from a range of compliance experts, private attorneys, and government officials on the latest federal export regulations and how best to navigate and comply with them. Before you spend the next two days discussing the various regulatory schemes, I thought it might be worth stepping back for a moment to remind ourselves why these laws were developed and why they're so important to our national security.

Most of these laws were developed in the second half of the 20th century, when the main national security threat was from foreign governments -- primarily the Soviet Union, the Eastern Bloc and other communist countries. We waged the Cold War to contain that threat, and these laws were an important part of that effort.

Starting in September 2001, the 21st month of this new century, we entered into a new war -- the war on terror -- which is a war mainly against terrorist groups that are not foreign governments. The threat posed by these groups is different from the symmetric threat of the opposing nuclear stockpiles of the Cold War. But it is just as dangerous -- and in some ways more dangerous. Given their suicidal fanaticism, the terrorists are less controllable and less predictable because they are impervious to the concept of mutually-assured destruction that restrains the actions of more rationally-thinking state actors.

While these foreign states and terrorist groups might differ in many ways, they have one very important thing in common -- which is that the threat they pose to our society, our people and

our allies is directly dependent on the destructive power they have at their control. And that destructive power is dependent, in turn, on the access they have to military equipment, weapons of mass destruction and dual-use technology that they can use against us.

- Our adversaries get that access in a number of ways:
- They purchase the weapons or technology directly from the producers;
- They develop the weapons themselves;
- They illegally acquire or steal the weapons lock, stock and barrel from others that have developed them;
- Or, they illegally acquire or steal the critical data, technological components or know-how that are the building blocks that they can then piece together into a final product.

Given that the US is the world's leader in advanced military technology; given that no adversary can match our industry in developing military goods and weaponry; and given that we have comprehensive regulatory schemes to keep those materials out of the wrong hands; it should come as no surprise that many of our adversaries try very hard to illegally acquire our technology. It should come as no surprise that America is the world's primary target for technology theft. And it should come as no surprise that -- as we speak here this morning -- our adversaries are busily at work in this city and throughout the US, seeking to acquire the technology that could be used to inflict damage on us and our allies. Somewhere there is a trade show of some kind where foreign experts are methodically searching out trade secrets to send back to their home countries. And somewhere, an American business is entering a joint venture with a foreign company -- the American company motivated by potential benefits of increased globalization and the foreign company motivated by potential access to sensitive American technology.

It really isn't possible to overstate the dimensions of this problem. A few statistics help to tell the story:

According to an Intelligence Community report from last year, there are private or public entities from 108 countries that are known to be involved in collecting sensitive, controlled U.S. technology -- a startlingly high number when you think that there are only about 200 countries in the world all in all. And, as to just one country -- the Peoples Republic of China -- the U.S. Immigration and Customs Enforcement (ICE) has launched more than 540 investigations of illegal technology exports to China since 2000 and the Defense Criminal Investigative Service has opened 143 such investigations in the past year alone.

The intensity of these technology acquisition efforts is matched by their craftiness and their ingenuity. Export violators use any number of methods to circumvent our technology transfer controls. In addition to the two that I've already mentioned -- attendance at trade fairs and joint ventures with American businesses -- we also see foreign governments using official delegations as platforms for illegal collection. In fiscal year 2005 alone, delegations from the few countries

that are the most flagrant violators requested a total of over 3000 official visits to military bases and/or defense industry facilities.

We see them using foreign students on occasion -- students who come to study in high-tech fields and thereby get exposure to our sensitive technologies. While the vast majority of foreign students come here to study without any criminal designs, a good number do, and it's no coincidence that several of the countries that send the most students happen to be the most active and determined collectors of our technology.

We see them using the internet. The Intelligence Community routinely finds evidence of foreign intrusions intended to acquire sensitive data.

And finally, we see them making regular use of the most traditional and direct approach -- which is simply to have a buyer call or email around and ask American companies to sell them controlled technology. They typically lie about the end-user, claiming the technology will be used domestically. On occasion, they find a company that unwittingly sells them the technology. But on other occasions, they find an individual or a company that wittingly and willingly succumbs to the temptation to skirt the export controls and make a buck.

II. The Response

These violations pose a concrete threat to America. And because of that, our enforcement agencies are responding with concrete law enforcement measures. From US Immigration and Customs Enforcement doubling the number of agents assigned to these cases to the 60% increase in our export control prosecutions over the past year -- we are seeing a steady crescendo in the intensity of our efforts against this illegal trade.

And these efforts are bearing fruit. In just the past month, we've seen charges or convictions in over ten different export control cases, including:

- the conviction of a Detroit man for trying to send night vision goggles, thermal imaging camera equipment and Boeing GPS modules to Hizballah;

- the filing of new charges against a scientist in Hawaii for plotting to assist China with development of its new generation cruise missile technology;

- And, the indictment of a woman in San Diego for conspiring with a Chinese agency to export accelerometers that calibrate the g-forces in nuclear and chemical explosions and have applications in the development of "smart" bombs.

III. The Initiative

To accelerate these enforcement efforts, last month we and our law enforcement partners announced a new national export enforcement initiative that has several features, all of which are designed to enhance our ability to attack this problem. In doing this, we are essentially following the blueprint we used to ramp up our counterterrorism efforts after September 11th.

First, we are expanding our training of field prosecutors around the country. Just as we made a concerted effort in the aftermath of 9/11 to train up our Assistant U.S. Attorneys in the complicated aspects of international terrorism cases, we are now making a push to build our prosecutorial expertise in the complexities of export control prosecutions.

The best thing we did along these lines was to appoint Steve Pelak as our National Export Control Coordinator to spread the gospel of export enforcement among our U.S. Attorneys' Offices. He is doing a tremendous job, and I know you'll be hearing from him when he speaks on a panel later in the conference.

As a second component of this initiative, we created Counter-Proliferation Task Forces in various judicial districts around the country. Just as we relied on Joint Terrorism Task Forces and other regional coordinating mechanisms in the counterterrorism context, we are establishing task forces that will bring together all the players -- the prosecutors, the investigative agencies, the export licensing agencies and the intelligence community -- to intensify our efforts against export theft in every region of the country.

Finally, we are raising the level of coordination between our national security prosecutors at DOJ and the export licensing officials at the State Department's Directorate of Defense Trade Controls and the Commerce Department's Bureau of Industry and Security. This ensures that we are effectively prioritizing and acting on those violations that are truly worthy and deserving of criminal investigation and prosecution.

IV. Implications for Industry and Attorneys

So what does all this mean -- or not mean -- for you, the in-house counsels, attorneys and compliance officers?

First, I want to stress that this initiative does not mean new regulations on your companies. We recognize, as you do, that international commerce is the lifeblood of our economy and that unnecessary over-regulation is not the answer to this problem. This initiative is focused on willful violations of criminal export laws -- nothing more and nothing less.

Nor does it mean any retreat from the value we place on voluntary disclosures by the industry. As I said, we will be working closely with our counterparts at State and Commerce. We will continue to support their voluntary disclosure programs and to take a favorable view of any corporation that makes full and honest disclosures to these entities.

This initiative does mean that you in the industry should have a greater opportunity to partner with us. We recognize that you are often the first ones to detect suspicious activity and that we need your help if we hope to get advanced warning of proliferation plots before they result in damage to our national security. The Commerce Department, the FBI and ICE each have industry outreach programs, and we will do everything we can to encourage them.

Finally, it means that you have a greater opportunity to provide input on how we can improve our efforts in this area. You have a tremendous amount of experience in this field, and all of us -

- myself, Steve Pelak, our colleagues at Main Justice and our partners in the task forces out in the field -- we all recognize that we need your guidance and your partnership if we are to be successful in safeguarding our technology and our protecting our national security.

Again, I'd like to thank the Practising Law Institute for inviting me to speak with you this morning. I've appreciated the opportunity to explain the national security concerns and objectives behind our export enforcement initiative. I'll be happy to answer any questions you might have, either from the podium or after I step down.

###