Testimony of Christopher Hankin
Former US Government official and
Senior Director of Federal Affairs, Sun Microsystems, Inc.
U.S.-China Economic and Security Review Commission
"Chinese Military Modernization and US Export Controls"
March 17, 2006

I thank the Commission for this opportunity to testify before you. Before I begin, I wish to clarify that I asked to testify today as a former US Government official not because of worries that what I might say could be restricted by my appearing as a representative of the US high tech industry. Rather, it is because certain facts began to establish themselves during my tenure at the US State Department from 1988-1994 that are highly instructive in contemplating effective US export control policy to China today.

As context, I wish to recall comments that then-Secretary of State Larry Eagleburger made in 1992 in a State Department "town hall" concerning the fall of the Soviet Union. He said that while he did not mean to sound nostalgic over the end of the Cold War, we did need to realize that our difficulties were far from over. While the Cold War was a more dangerous time, it was likely going to prove a far less complicated time. He predicted – rightfully – a complicated world of enhanced regional, religious, and ethnic conflict.

It is this more complicated world that the US export control system is still adapting to.

What are these facts from the 1988-1994 period that I find so instructive?

4 FACTS FROM THE PAST.

1. COCOM is dead, and it will not be replaced.

I cannot overemphasize the importance of this fact. The Coordinating Committee for Multilateral Export Controls (COCOM) had an agreed target – the Warsaw Pact and China. It had an agreed, specific, targeted mission – maintaining and expanding the qualitative edge of our military over the Soviets, in recognition of their quantitative edge. It had an agreed and enforceable licensing policy over arms and dual-use exports to the targeted countries – enforceable through The US Government's ability to veto other nations' proposed exports. The US had intelligence on the Soviet military's high-tech shopping list, and had used this to shape an agreed list of controlled items.

The Wassenaar Arrangement only replicates the agreed list of controlled items. Why we have ended up with such an inadequate replacement was not the fault of our negotiators., but for other reasons, most particularly the disappearance of the agreed threat. A good, brief discussion of this can be viewed at http://www.armscontrol.org/act/2005_11/NOV-LOOKINGBACK.asp.

2. WMD proliferation does not require high technology.

A frustration grew in the Reagan Administration, and continued into the Bush Administration, that Iraq was acquiring useful western technologies for both its military and its WMD programs despite controls imposed pursuant to COCOM, the Australia Group, the Missile Technology Control Regime (MTCR), and the Nuclear Suppliers Group. The first, while controlling a long list of items, was irrelevant to Iraq. The other three groups, while global in scope, imposed control lists that were (rightfully) targeted to items of most concern. This inability to prevent WMD-useful, but not critical, exports became acute on a proposed purchase that the US exporter brought to the attention of the US government. While the item was not a controlled item, the exporter was concerned that the purchaser might be intending to use it for WMD purposes. The US government agreed, but did not have clear authority to block the export. The result was the creation of the "Enhanced Proliferation Controls Initiative" (EPCI), controls built around end-use and end-users rather than around the performance level of any particular item.

3. While unilateral controls have their place, they are not effective security tools.

After the first Iraq war, it was clear that Iraq's WMD programs and conventional military had been well supplied by the Russians, Chinese, and the Europeans. We had the satisfaction of knowing that our soldiers had not faced US-made weapons nor technology on the battlefield. Congressman Sam Gejdenson used to call this the satisfaction of knowing you didn't "trade with Hitler." But Congressman Gejdenson also recognized that such unilateral controls should not be confused with controls having any possibility of actually preventing an adversary from acquiring the capability of concern. Unilateral controls can make a useful political or foreign policy statement, but they do not provide adequate national security protection and it is dangerous to pretend otherwise.

4. Exporters must police themselves for export controls to be effective.

With COCOM, very little benign trade was impacted, and to the extent it was, I'm not so sure those of us in the US government were terribly upset about it! But those days are over. Today, the volume of global trade that must be screened for proliferation, embargo and other concerns is monumental. There is no way that the US government can monitor all this trade. Our government has become hugely reliant on US exporters to police themselves. And this means these companies must have extensive, clear internal compliance programs imposed on their sales forces and their e-commerce websites. Such programs cannot be based on fuzzy lines or parameters. Policy throughout the company must be black and white – which becomes especially acute and difficult on end-use and end-user controls.

NOW ON TO TODAY.

With this as background, now let me speak with both my hats: as former government official and as an employee of Sun Microsystems, Inc.

Sun is a world leader in networked computer systems, providing scalable computer and storage systems, high-speed microprocessors and a comprehensive line of high performance software for network computing equipment. Sun's revenues come to roughly $14 Billion per year. We operate in all major markets worldwide, and well over half of our sales occur outside the US.

China is an important market for Sun; we do over $300 million in sales in the PRC. While a large figure, it is also important to note that the PRC has one of the fastest growing economies in the world, meaning that there is substantial potential for growth in our business there as well.

Export controls have historically been an important factor in our presence in China, affecting every dimension of our business there. As Sun does not produce military products, controls that affect us in China are primarily those relevant to "dual-use" civilian products and technology.

Export controls affect not only our sales of computers to customers in China, they regulate our provision of software, determine how we manage our internal networks and communications, impact the choice and design of our facilities, and have a role in our hiring practices. Moreover, as export controls on China also apply to PRC nationals living abroad, their impact extends to our operations around the globe.

In the time of COCOM, export controls primarily affected items rarely traded to a group of nations that did not enjoy significant deal of economic interaction with the West, or with the United States. This is not the case today with the PRC, creating a historically unique set of circumstances for US business. On the one hand, China represents a significant and growing export market for US products, including high technology. On the other, export controls must be a consideration in every transaction in that market, and must be administered flawlessly and at great expense by US high tech companies.

To say that US export controls affect every Sun transaction in the PRC market is not exaggeration for effect; it is a simple statement of fact. The export licenses that are required for shipment of high-end computers are now a very small part of Sun's export control management in the PRC.

"Catch-all" controls are a prime example of the comprehensive impact of export controls on business activities in China. Since the inception of the previously-referenced EPCI, every US-origin product or technology, regardless of its relevance, shipment volume, or low-cost, is controlled for export to the PRC if is shipped to a proliferation entity. While this restriction is seldom enforced on items such as auto parts or hand tools, it could be, and companies are obliged to construct complex and costly screening programs to ensure that none, repeat none, of their products end up in the hands of a "proliferation entity."

And what is a "proliferation entity?" A few are listed by the Government, and others are publicly known, presenting no problem for high tech exporters, who routinely screen each transaction, from the 50 cent cable to the million dollar computer, against a list of proscribed entities and individuals. The problem arises where there is little or no data on a particular customer (for example in an electronic commerce transaction) or where the status of an entity is not clear. This is the case in many of the thousands of transactions that a company like Sun conducts (and screens) on a monthly basis in China.

A typical example of this kind of problem involves sales to a university. Large universities in the PRC are major buyers of information technology products. However, as in the U.S., some universities have contracts with the government for various types of research, some of which might involve activities that would be prohibited under EPCI.

As the entire scope of all university activities may not be known or even impossible to determine by a U.S. vendor, the only risk-free course is not to make the sale. Ultimately this benefits the non-US company who is willing to step in, or a US competitor with a less disciplined approach to export controls.

I need to emphasize this again- in the many circumstances where there is insufficient information on a customer, or where high volume or low value of a transaction makes collection of more data impossible, the “default” of US high tech businesses must be to avoid the transaction. Ironically, this loss of business is most likely in transactions involving items of no strategic value at all.

The extension of this “catch-all” approach is even more problematic when applied to “military” end-uses in China. The “military” in China can be involved in a very wide variety of activities, ranging from the distribution of foodstuffs to the provision of security at airports or at the upcoming Olympic games. Imposition of such a requirement for all or most U.S.-origin items exported to China would result in companies deciding they have to simply embargo military entities. Which in China will then lead to very difficult screening and decision-making as regards end users, as issues such as co-location, financial relationships, contract/consulting activities and others ensure that a very wide range of economic actors are potentially “military” end users.

All this is made more problematic by the fact that our allies do not intend to impose similar catch-all controls on military end users in China. The possible impact of such an extension could be a burdensome and unilateral control that: (1) gives a false sense of the government having taken effective action; (2) requires finite government and corporate resources be devoted to compliance activity that could be more properly targeted on potential exports and espionage of far greater importance; and, (3) hands the Chinese government an easy talking point to use against the US government in the very important negotiations over Chinese barriers to US high tech exports.

When considering the issue of US export controls on China, we cannot overemphasize the value of multilateralism. It is an accepted principle that multilateral controls are more effective than unilateral controls, but we must be wary of pointing to superficial similarities in controls as evidence that U.S. versions are multilateral and thus effective national security tools. Wassenaar is no COCOM. We have no assurance through Wassenaar that others are controlling dual-use technology as tightly as the US, and indeed we know in fact there is little consensus in the international community on specific strategic threats posed by China.

4 RECOMMENDATIONS.

I would like to advance a number of positive steps that could greatly enhance the partnership between US Government and business in managing a smart control system:

- **Think multilateral, not unilateral.**

If the purpose is national security, then the most important ingredient to the success of the control is adequate multilateral implementation.

- **Rather than "catch-all" controls, promote more extensive use of listing and "is informed" procedures.**

It is important that information available to the US Government be made available to companies operating in China, and that adverse intelligence identifying bad end-users be published. This includes cases where the Government initially "informs" an individual exporter of such intelligence. This will enhance the odds that the bad player does not obtain the desired item, and places all competitors on a level playing field.

- Enforce more technical focus on the list development process.

Not all items are equally useful for military and proliferation projects; items should be controlled on the basis of features that are of particular use to an identified military mission.

- Provide specific recognition of company internal control programs in developing controls and in enforcing them.

US high tech companies doing business in China manage extensive and complex export internal control programs. The success of US export controls is highly dependent on their existence and effectiveness. More can be done by the US government to recognize and leverage these programs.

I will be happy to respond to questions from the Commissioners.