March 17, 2006
Statement by

John J. Tkacik, Jr.
Senior Research Fellow in Asian Studies
The Heritage Foundation

Before the
The U.S.-China Economic and Security Review Commission

Hearing on Chinese Military Modernization and Export Control Regimes

I thank the Commission for its invitation to testify this morning on U.S. export control regimes aimed at China.

Introduction

The United States, alone among the technologically advanced nations, has in place regulations that limit the export to China of dual-use as well as military items, services and technologies across a broad spectrum; and the U.S. alone has regulations in place that restrict the participation of Chinese personnel in advanced research in dual-use areas.

Since the Tiananmen crackdown of June 1989, the European Union has maintained a prohibition on the transfer of lethal military equipment to China, and individual EU member states have separate statutory bans on arms sales to various countries reflecting national arms transfer policies. The EU has indicated, however, that it intends at some point to lift those bans -- particularly if China's human rights behavior improves.

The United States is one of only two major world powers that now considers China to be a credible and potentially imminent military threat; the other is Japan. Additionally, Taiwan also suffers under China's military and political pressures and accordingly has even tighter technology controls on China than does the U.S. In recent years, Japan has indicated some willingness to join the United States in restraining high-technology exports to China.

For the United States, however, simply having regulations in place is not sufficient. Those regulations must be enforced and when export licenses are granted, a high percentage of those licenses must undergo post-licensing inspections and follow up by competent personnel.

Export controls, however, cannot not simply be a matter of monitoring and restricting the export of equipment and technology documentation. They must also include watching those who have access to that technology in the United States. In April 2002, the General Accounting Office (GAO - now the Government Accountability Office) reviewed semiconductor export licensing procedures, and in September 2002, the GAO reviewed "deemed export" licenses for foreign personnel -- seventy percent of them for Chinese

nationals -- to engage in research in restricted areas. Both these reports were comprehensive, probing and I believe compete -- and both revealed an across-the-board failure of the export administration bureaucracy to administer adequately its own regulations.

"Deemed Exports" and Industrial Espionage

Two decades ago, when I supervised the issuance of student and exchange visas for China, U.S. visa officers learned that most Chinese student visa applicants were indoctrinated by their work units, schools or local public security service precinct stations about their responsibilities to the motherland while in the United States. From all reports, I believe this is still the case. It was and is my impression that Chinese security officials inform all Chinese science and technology workers visiting the U.S. that they could be given specific collection tasks while in the U.S. The case of two Chinese academics at American University, Ms.Gao Zhan and her husband, Xue Donghua, is instructive. Apparently, Ms. Gao and Mr. Xue had received such a tasking and reportedly managed to export as much as $1 million in radiation-hardened microchips to a military laboratory in Nanjing before being arrested in 2001. Although the couple evinced a desire to cooperate with U.S. government investigators, as of January 2006, the Department of Homeland Security had reportedly petitioned to have them deported back to China.

Gao and Xue were emblematic of vast Chinese government effort to collect industrial and technical secrets. A year ago, in March 2005, FBI Assistant Director Dan Szady, commented on the existence of an estimated 3,000 Chinese front companies operating in the United States in order to facilitate illegal technology transfers to the Chinese government. In September, Michelle Van Cleave, the national counterintelligence executive, told the House Judiciary subcommittee on immigration, border security and claims that Chinese "state-directed espionage remains the central threat to our most sensitive national security technology secrets." She said Chinese intelligence agents are "very aggressive" in business and "are adept at exploiting front companies." Chinese intelligence assets in the United States "take advantage of our open economic system to advance China's technical modernization, reduce the U.S. military advantage and undermine our economic competitiveness."

Nor is the United States the only target of Chinese industrial espionage. Last May, the French newspaper *Le Monde* identified a Chinese front group known as "The Chinese Students and Scholars Association of Leuven" in Belgium that coordinated industrial espionage in several northern European countries. A few weeks earlier, a 22-year-old Chinese woman was accused of industrial espionage against a major French industrial firm -- she had six computers and two hard drives filled with industrial data from the firm's research and development division where she had been working as a student intern.

These are only a few examples of literally scores of published reports in the last five years of incidents of state-sponsored Chinese industrial espionage around the world.

It is perfectly reasonable, therefore to "deem" that technology exposed to a Chinese national researcher, scientist or engineer is in fact an "export" to China for the purposes of the Export Administration Act. Under present guidelines, however, it is responsibility of the U.S. firm or institution that makes such "deemed exports" to apply for an export license. I have the uneasy feeling, based on the September 2002 GAO report, that most have no idea of their responsibilities.

Semiconductor Technology

I do not have the time -- or the expertise -- to discuss the full spectrum of dual-use technologies that are covered by export licensing laws. I have studied China's semiconductor sector, however, and have a few thoughts I would like to share with the Commission.

In the case of semiconductor export licensing, at least, the export licensing bureaucracy seems hopelessly at sea. The April 2002 GAO report documented statements from several U.S. government officials that export controls for China followed a basic "two generations behind" rule-of-thumb banning semiconductor manufacturing equipment (SME) sales. That is, any SME items less than two-generations behind the state of the art in the United States would not be approved for export to China.

However, when the GAO sent its draft report out for comment to U.S. agencies, officials throughout the licensing bureaucracy -- in Defense, State and Commerce departments -- denied that the "two generations behind" guideline existed and that in any event, the disparity of different SME systems and components made it difficult to quantify the "two generations" guideline. Moreover, the GAO documented that, even though export control officials had privately admitted that there was such a rule, written or not, it apparently did not govern their licensing decisions.

And in the case of "deemed exports" the bureaucracy admitted that it had approved all but three of 602 applications in the year 2001 for Chinese personnel to work in sensitive technologies (mostly in telecommunications and semiconductor research) albeit with certain caveats on access to sensitive research and technology. But in no case was there any reported follow-up to ensure that the stringent conditions on the license approvals had been followed.

This was the case as of 2002 -- and there seems to have been little improvement in the situation since then. No doubt the Commerce Department which houses the Bureau of Industry and Security is under tremendous pressure from U.S. exporters for relaxed enforcement. Here, I think we can see the major disconnect in America's export control ethos.

Now, I do not wish to demonize US businesses for acting in what they viewed as their own short-term interests. U.S. exporters seem to think that the government knows all the secrets of industrial espionage, and that if the situation were really serious, the U.S. government would not bend to their pressure no matter how sharp it might be. And the

Commerce Department, in particular, seems to view businesses as its natural constituency and thus acts as their advocate in interagency export control deliberations. But clearly, if some future catastrophe results from the transfer of sensitive technology to China, the American people (and the Congress) are more likely to blame Commerce Department which failed adequately to administer its regulations, not the businesses that pressured it.

And a catastrophe could erupt, but it will likely be a slow eruption over a long period of time. Although America's defenses rely on the superiority of its "network centric" weaponry, which in turn relies on the superiority of American microchips, that superiority is eroding -- in large part because of a lack of recognition of the potential challenge from China in this area.

Since 1986, the technology gap between U.S. and Chinese semiconductor manufacturing capacity has narrowed almost to zero. The current industry standard semiconductor fabrication dimensions are now around 0.18 and 0.13 micron line-widths, and Chinese wafer-fabs already produce DRAMS with these design rules. The current U.S. state-of-the-art is now 0.09 microns -- or 90 nanometers -- and at least one Chinese fab is said to be installing a 90 nanometer production line now. U.S. semiconductor manufacturers are now working on 65 nanometer design rules -- in concert with a French fab.

In February 2005, the Defense Science Board issued a report on "High Performance Microchip Supply" which -- to me at least -- seemed focused on the security challenge posed by the explosion in Chinese microchip design and production and th eimpact on America's strategic position. Alarmed by the leakage of U.S. technology to China, the DoD report even proposed bilateral Wassenaar-type agreements with Japan and Taiwan on SME exports to China. Incidentally, the DoD report also bemoaned the fact that Commerce Department microchip export rules are always out of date, and hence there is business pressure on the licensing offices to bend their own rules to "keep up with the times."

According to the Defense Science Board report, the strategic threat to the United States in the semiconductor sector is significant in two contexts: 1) the globalization of the microchip supply chain is draining production capacity from the United States and in a crisis it would be difficult to ramp up domestic output; 2) there is a real threat that microchip supplies from overseas -- particularly from China -- would be untrustworthy; that "opportunities for adversaries to clandestinely manipulate technology used in U.S. critical microelectronics applications are enormous and increasing."

In other words; not only is the Pentagon finding fewer and fewer sources for application specific integrated circuit microchips for highly classified defense applications (such as signals processing, encryption, guidance systems, etc.) but the US military already relies heavily on China for the unclassified laptops and PCs that are the bulk of the nervous system of our network-centric warfare doctrine. It is all well and good to say that the US simply won't buy Chinese-made computers for our military, but what happens when the global supply-chain means all laptops and PCs have some Chinese components in them?

Simply answering that 70 percent of China's advanced technology exports are made by non-Chinese companies is inadequate. As microcircuitry architecture becomes orders of magnitude denser than today, it becomes ever easier to hide lines that serve as Trojan Horse circuit designs, radio-frequency receivers and other "backdoors" to circumvent encryption, muddle signals, induce data failure and the like.

Are Chinese semiconductor firms capable of such chicanery? Chinese advanced technology companies have already proved themselves adept at down-loading and pirating tapeouts and masks that have been sent to contract fabs for mass production. And there are already several hundred semiconductor design labs in China -- sponsored and paid-for by foreign firms including America's top microchip corporations. While one American semiconductor design engineer told me this week that he did not think the Chinese designers he worked with were "smart enough" to handle the task of sabotaging circuit maps, he admitted that his Israeli colleagues were.

This is hardly reassuring. I suspect that US-sponsored semiconductor design labs in China lose engineers as they gain experience only to have them replaced by inexperienced engineers in need of new training. No doubt, experienced engineers are siphoned off by Chinese government, military and academic units to work on more advanced projects.

Case Study: SMIC

Export controls that ban advanced-technology SME exports to Chinese government and military end-users but permit exports to so-called "foreign-owned" end-users are self-defeating. SMIC in Shanghai, for example, is considered to be a "foreign-owned" microchip foundry fab. The Taiwan-invested "Semiconductor Manufacturing International Corp." (, SMIC), was launched in Shanghai in 2000, reportedly with private funding. The US$1.48 billion venture, however, seems to be a totally Chinese government-controlled operation. Its president, Richard Chang once complained mightily to the media about the strictures Beijing placed on the company as it was raising venture capital. In October 2001, Chang told the *Financial Times*, "the authorities said how much money we could borrow, and from which Chinese banks - this is very new to us." Said the FT, "Chang has noticed another difference to doing business in China compared with Taiwan; he had had to employ 11 public relations officers to keep local officials informed, compared to just one in Taiwan."

One wonders what these PR people do. SMIC's website (http://www.smics.com) carries some useful information -- it does disclose that SMIC's Chairman is a Chinese government official ("Yang Yuan Wang is also the Chief Scientist of the Microelectronics Research Institute at Beijing University. He is a fellow of the Chinese Academy of Sciences and The Institute of Electrical and Electronics Engineers").

In 2002, SMIC reportedly purchased five 257-nanometer (roughly 0.25 micron) lithography machines made by ASML of Netherlands, giving SMIC access to levels of technology for which the United States, at that time, still refused export licenses. U.S.

guidelines reportedly limited the export to China of lithography equipment with capabilities finer than 0.35 microns, although Motorola was granted a license to produce chips at its MOS-17 fab in Tianjin, China, with 0.25 linewidths. In October 2003, however, Motorola abandoned its MOS-17 plant, into which it had already sunk $1 billion, swapping it to SMIC for a 10% share in SMIC -- a deal that market-watchers estimated was a loss of about 90 cents on the dollar. In February 2005, Motorola sold its SMIC shares expecting to raise about $115 million.

Over the past five years, SMIC advanced to 0.13-micron production (in 2004) and introduced 0.18-micron silicon germanium (SiGe) production technology (in 2005). In January 2006, SMIC and the German firm Infineon signed an MOU that will transfer Infineon's "leading 90nm DRAM trench technology and 300-mm production know-how to SMIC, with the flexibility of further transferring its 70nm technology in the future. In return, SMIC will manufacture products in this technology exclusively for Infineon."

But for all this money and effort, the SMIC investment still does not seem to have been well thought-out, particularly in the 2001-2004 worldwide economic slump when most customers purchased their chips only from reliable suppliers.

Either that, or perhaps SMIC was not intended to compete in the international chip market in the first place. By September 2002, SMIC admitted it was headed for large losses. In order to keep their production lines running, both SMIC and Grace have resorted to turning out low-end DRAM chips. Yet by April 2003, one Shanghai-based semiconductor expert told reporters "I think they'll rack up incredible losses in DRAM . . . [SMIC is] building production lines, but they have no customers." SMIC's lack of customers persists despite a growing demand for chips by foreign firms in China. In March 2003, most international semiconductor companies remained puzzled by the nature of China's chip sector. Infineon's CEO Ulrich Schumacher, commented "China is this big phenomenon. Is it the biggest market of the future? Or is it the biggest threat? Nobody has a clue what China really is. What do you do now?"

Schumacher's head-scratching did not prevent Infineon from providing SMIC with advanced SME in return for DRAM output. After three years of operations, SMIC is still a money-loser, posting $15 million in losses at the end of 2005. But SMIC apparently is a money-maker for the Chinese government, which apparently has recouped a good deal of its investment by selling stock shares and depository receipts on Hong Kong and U.S. bourses.

And in 2005, SMIC also offered to buy a half-billion dollars worth of semiconductor manufacturing equipment from the American SME-giant, Applied Materials -- provided it could get a full loan guarantee from U.S. taxpayers via the US Export-Import Bank.

In the event, the EXIM Bank loan guarantee application was denied in March 2005 amid heated complaints from U.S. businesses, but the episode reveals the ironic sides of U.S. export controls. On the one hand, we deny licenses to Chinese military and state-owned companies for this equipment. On the other, we consider giving U.S. government loan

guarantees to companies that -- to all appearances -- operate under the control of the Beijing regime. By the same token, in 2001 the U.S. government approved export licenses for 0.25 micron design-rule SME at the Motorola MOS-17 fab -- only to have Motorola sell off the plant several years later (and at a significant financial loss) to SMIC.

Clearly, semiconductor export control guidelines in place for China are not taken seriously either by Chinese firms or, apparently, by the U.S. bureaucrats who are supposed to enforce them.

Conclusion

Are existing U.S. semiconductor export control regulations and guidelines for China fixable? Because the technology is moving fast, and because the U.S. has not yet completely lost its technology edge in semiconductors, I think so. But fixing the problem requires an entirely new enforcement mentality. This means that perhaps dual-use export controls for China should reside somewhere else in the bureaucracy rather than in the Commerce Department -- the Pentagon or Department of Homeland Security come to mind.

It also means that the "two-generations-behind" rule should be codified and adhered to rigidly and a cadre of engineers with expertise in semiconductors should keep a current talley of just what the state-of-the-art is at any given time. It also requires that very strict end-user and re-export restrictions be accompanied by rigorous inspections and, when necessary, criminal prosecutions or meaningful trade sanctions.

Of course, one vociferous (and persuasive) objection to SME export controls is that "if we don't sell it, some other country will." However, with Japan and Taiwan as two major world suppliers of SME, and two major countries in East Asia that are not afraid to admit they see a "China Threat", there is a very real opportunity for the United States to coordinate export restrictions with those two countries, and through them, to exert our influence on European suppliers to follow suit. The Defense Science Board recommended this last year, and I believe it is a feasible measure.

On "deemed exports", I believe that the U.S., Japan and Taiwan could also be prevailed upon to coordinate deemed export license policies. But at the very least, the U.S. should actually deny applications for nonimmigrant Chinese personnel to gain access to advanced semiconductor research in the United States, and not simply lade approvals with unsupervised conditions that are supposed to insulate sensitive research from prying eyes.

Finally, the Congress and the American people should be apprised of the serious erosion of America's semiconductor superiority. Without a national consensus that this erosion must be slowed in the interests of national security, export-licensing restrictions on China will become an empty exercise.