STATEMENT OF

MAYNARD C. ANDERSON

HOUSE OF REPRESENTATIVES COMMITTEE ON THE JUDICIARY

SUBCOMMITTEE ON IMMIGRATION, BORDER SECURITY & CLAIMS

SEPTEMBER 8, 2005

In the 1985 report entitled, "Keeping the Nation's Secrets," The Stilwell Commission wrote that given the extraordinary importance of advanced technology to our nation's military capabilities, its loss to a potential adversary -- by espionage, theft or other unauthorized disclosure -- can be crucial to the military balance.

That is perhaps more true today. There is a great deal of support for the assumption that national security and economic strength are indivisible. Both military and economic security will depend on effective countermeasures. United States economic competitiveness is a national security issue. However, as attempts are made to ensure proper protection to truly sensitive information and technology, the competitive position of American industry in the world market must be maintained. Care must be taken to balance control with tolerance for contributions to technology development.

The United States produces more intellectual property than any other nation and, in the opinion of many, does the poorest job of protecting it. Efforts to acquire unclassified technology by illicit means is common partly because the risk of exposure and severe penalties to the perpetrators are much lower than conventional espionage. And, those who seek our protected information have generally been described as "adversaries" or potential adversaries. It is more likely that the greatest challenge to the United States technology and industrial base comes from United States friends and allies. One of the most expedient and least expensive ways for any nation to increase its industrial capability is by theft from the United States, the most lucrative target in the world. Our competitors are not unaware that the real test of success in this world of military and economic supremacy may not be who first develops technology but rather who is first to use it effectively.

As an "Open Society," the United States offers invited or illegal visitors almost unlimited opportunities to take advantage of our accomplishments. Large numbers of immigrant workers along with foreign exchange students and visitors, combined with a perception

on the part of some of our citizens that there is a lesser threat, contribute to the vulnerabilities of our technology. The foreign collectors are not necessarily to blame. Our open society citizens have what might be called a "frontier mentality". When strangers come, they are offered assistance, invited stay for food or overnight. This is part of the American character in many parts of the country and is not necessarily bad. However, the risks must be understood. It is necessary to think and talk about risks like this. Corporate espionage is often an unreported crime. It is hard to admit that someone has taken advantage of a situation we created, but we need to confess so corrective actions can be developed. Corporate espionage is not an insignificant issue. A recent report by Provizio, Inc., "Counterintelligence for Today's Fortune-1000 Company," notes that the cost to United States companies from lost proprietary information in 2005 is $133 Billion. This data is based only on reportable, quantifiable losses through corporate espionage and "social engineering." The National Counterintelligence Executive estimated the 2004 economic espionage loss at $300 Billion.

It is reasonable to assume that in the future, there will be amorphous threats that are difficult to define sometimes because they will come from an array of national and stateless entities. As new alliances and friendships among nations develop and change, there will be a need to be leery that a euphoria of cooperation might conceal sinister purposes, intent, and capabilities that put us at a disadvantage.

Aside from the common situations in which foreign entities are able to obtain our technology -- the graduate student who serves as a no-cost assistant to a professor doing research in a target field; foreign employees of American firms abroad; ethnic targetting; open data bases; creation of front companies; overt sponsorship of research activities in the United States -- there are nontraditional threats such as ethical failures on the part of trusted personnel. There are those individuals who are prepared to traffic in information and knowledge because they are greedy and susceptible to foreign pressure. They bolster the claim by Robert Louis Stevenson who alleged that "everyone lives by selling something."

In summary, John. J. Fialka, "War by Other Means: Economic Espionage in America," wrote that "America may have won the Cold War but we are losing ground economically to those who pilfer our commercial secrets."

Moving from prediction to prescription, efforts must be made to more clearly determine what technology can be shared with other nations without damage to our national interest, and how best to protect those genuinely critical technologies in times of limited resources. It would seem reasonable to conclude that the degree of protection should be determined by the cost of unauthorized disclosure which, in other words, would be a damage-based system. If there were standards of value related to sensitivity, American industrial executives would better identify the return on investment of security costs. Such a system would also serve to heighten awareness of the costs of compromise and improve accountability for their actions on the part of the technology custodians.

H. L. Mencken wrote that "It is not nice to think evil of others but it is often wise."

Following that guidance, we must conclude that United States technology remains at risk and the United States is a lucrative source for foreign collectors. Other nations use virtually every means available to obtain our achievements.

As technology advances, seemingly beyond our ability to develop mechanisms for its protection, there should be established a unified program of technology protection. Integration of management, protection, and utilization of technology is an objective.

Both developers and users of technology should be equipped with mechanisms to ensure the security of their people, facilities, systems, and information - the real treasures of the 21st Century.

Stopping the foreign acquisition of our technology in ways that are both effective and appropriate in our open society is one of the most urgent and complex issues facing us today. Not because it is right in an academic or idealistic sense, but to ensure the national security of the United States and to advance the national interest.

To better protect critical technologies from foreign collectors, the following recommendations are offered:

1. Conduct a review of appropriate laws to determine the need for additional legal protections. For example, consider authorizing payment of rewards to persons who provide information leading to an arrest for economic espionage or the identification of foreign collection agents.

2. Consider enactment of legislation to enhance criminal enforcement remedies against civilian employees of the government or employees of contractors who disclose protected information without authority.

3. Consider enactment of legislation that would protect against the export of sensitive information or technology to another nation unless that nation can prove its intent and capability to protect the information.

4. Establish international security standards applicable to offshore contracts where a foreign contractor or supplier may acquire access to our protected information.

5. Utilize existing legal remedies to withhold payments under government contracts in order to obtain United States contractor compliance with security requirements.

6. Specify a uniform requirement for government and contractor employees to report all contacts with foreign nationals who request classified or unclassified national security information, or which suggest a possible effort at recruitment, and report all official or unofficial contact with any foreign national of any country determined by appropriate authority to have interests inimical to the United States.

7. Consider imposing a requirement that all foreign students in the United States be required to execute a form like the SF 86 (a personnel security form that contains background information on individuals) as well as financial disclosure forms in order to ensure that there is a basis on which the individual's affiliation and support can be determined. Failure to submit the requrested information could serve as grounds for visa termination and deportation.

8. Cause a review of the Freedom of Information Act (FOIA) to determine whether certain provisions should be strengthened or eliminated.

9. Ensure that proper technology protection criteria is included in contracts between industrial firms and the United States Government with particular emphasis on those contracts with the Department of Defense.

10. Ensure that government counterintelligence elements are funded, organized, trained, educated and tasked to take appropriate actions to assist government agencies and industry in combatting economic espionage, illicit technology transfer, and improper use of critical and dual technologies by government and industry.

11. Order the development of a strategic plan for technology management which will map the road to the future and will ensure that custodians are not required to protect insignificant technology. Such a plan would ensure that standards of protection are based on the relevance of product desirability to threat of loss and the vulnerability to collection efforts. In other words, does any other nation have the technology in question, and does any other nation want it?

12. In coordination with representatives of the insurance industry, determine the feasibility of insuring specific critical technologies against the risk of loss, compromis, or unauthorized disclosure.

13. Develop continuing evaluation programs for personnel with access to technology and those involved with technology management. This should include companion security awareness and training programs which reinforce the responsibilities and accountability of all personnel for protection of significant information.