SOURCES AND METHODS OF FOREIGN NATIONALS ENGAGED IN ECONOMIC AND MILITARY ESPIONAGE

HEARING

BEFORE THE

SUBCOMMITTEE ON IMMIGRATION, BORDER SECURITY, AND CLAIMS

OF THE

COMMITTEE ON THE JUDICIARY
HOUSE OF REPRESENTATIVES

ONE HUNDRED NINTH CONGRESS

FIRST SESSION

SEPTEMBER 15, 2005

Serial No. 109–58

Printed for the use of the Committee on the Judiciary

Available via the World Wide Web: http://judiciary.house.gov

U.S. GOVERNMENT PRINTING OFFICE

23–433 PDF WASHINGTON : 2005

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

COMMITTEE ON THE JUDICIARY

F. JAMES SENSENBRENNER, JR., Wisconsin, *Chairman*

HENRY J. HYDE, Illinois
HOWARD COBLE, North Carolina
LAMAR SMITH, Texas
ELTON GALLEGLY, California
BOB GOODLATTE, Virginia
STEVE CHABOT, Ohio
DANIEL E. LUNGREN, California
WILLIAM L. JENKINS, Tennessee
CHRIS CANNON, Utah
SPENCER BACHUS, Alabama
BOB INGLIS, South Carolina
JOHN N. HOSTETTLER, Indiana
MARK GREEN, Wisconsin
RIC KELLER, Florida
DARRELL ISSA, California
JEFF FLAKE, Arizona
MIKE PENCE, Indiana
J. RANDY FORBES, Virginia
STEVE KING, Iowa
TOM FEENEY, Florida
TRENT FRANKS, Arizona
LOUIE GOHMERT, Texas

JOHN CONYERS, JR., Michigan
HOWARD L. BERMAN, California
RICK BOUCHER, Virginia
JERROLD NADLER, New York
ROBERT C. SCOTT, Virginia
MELVIN L. WATT, North Carolina
ZOE LOFGREN, California
SHEILA JACKSON LEE, Texas
MAXINE WATERS, California
MARTIN T. MEEHAN, Massachusetts
WILLIAM D. DELAHUNT, Massachusetts
ROBERT WEXLER, Florida
ANTHONY D. WEINER, New York
ADAM B. SCHIFF, California
LINDA T. SÁNCHEZ, California
CHRIS VAN HOLLEN, Maryland
DEBBIE WASSERMAN SCHULTZ, Florida

PHILIP G. KIKO, *General Counsel-Chief of Staff*
PERRY H. APELBAUM, *Minority Chief Counsel*

SUBCOMMITTEE ON IMMIGRATION, BORDER SECURITY, AND CLAIMS

JOHN N. HOSTETTLER, Indiana, *Chairman*

STEVE KING, Iowa
LOUIE GOHMERT, Texas
LAMAR SMITH, Texas
ELTON GALLEGLY, California
BOB GOODLATTE, Virginia
DANIEL E. LUNGREN, California
JEFF FLAKE, Arizona
BOB INGLIS, South Carolina
DARRELL ISSA, California

SHEILA JACKSON LEE, Texas
HOWARD L. BERMAN, California
ZOE LOFGREN, California
LINDA T. SÁNCHEZ, California
MAXINE WATERS, California
MARTIN T. MEEHAN, Massachusetts

GEORGE FISHMAN, *Chief Counsel*
ART ARTHUR, *Counsel*
ALLISON BEACH, *Counsel*
LUKE BELLOCCHI, *Full Committee Counsel*
CINDY BLACKSTON, *Professional Staff*
NOLAN RAPPAPORT, *Minority Counsel*

CONTENTS

SEPTEMBER 15, 2005

OPENING STATEMENT

Page

The Honorable John N. Hostettler, a Representative in Congress from the State of Indiana, and Chairman, Subcommittee on Immigration, Border Security, and Claims 1

The Honorable Sheila Jackson Lee, a Representative in Congress from the State of Texas, and Ranking Member, Subcommittee on Immigration, Border Security, and Claims 2

The Honorable Zoe Lofgren, a Representative in Congress from the State of California, and Member, Subcommittee on Immigration, Border Security, and Claims 5

WITNESSES

The Honorable Michelle Van Cleave, National Counterintelligence Executive, Office of the Director of National Intelligence

Oral Testimony 7

Prepared Statement 10

Dr. Larry Wortzel, Visiting Fellow, The Heritage Foundation

Oral Testimony 19

Prepared Statement 21

Mr. Maynard Anderson, President, Arcadia Group Worldwide, Inc., and former Deputy Under Secretary of Defense for Security Policy

Oral Testimony 23

Prepared Statement 25

Dr. William A. Wulf, President, National Academy of Engineering, The National Academies

Oral Testimony 30

Prepared Statement 34

APPENDIX

MATERIAL SUBMITTED FOR THE HEARING RECORD

Map on the "Number of Patent Applications and Foreign Students Per County," submitted by the Honorable John Hostettler, a Representative in Congress from the State of Indiana, and Chairman, Subcommittee on Immigration, Border Security, and Claims 57

Prepared Statement of the Honorable Sheila Jackson Lee, a Representative in Congress from the State of Texas, and Ranking Member, Subcommittee on Immigration, Border Security, and Claims 58

New York Times Article submitted by the Honorable Zoe Lofgren, a Representative in Congress from the State of California, and Member, Subcommittee on Immigration, Border Security, and Claims 59

The National Counterintelligence Strategy of the United States, submitted by the Honorable Michelle Van Cleave, National Counterintelligence Executive, Office of the Director of National Intelligence 61

Revised Prepared Statement of Dr. Larry M. Wortzel, Visiting Fellow, The Heritage Foundation 75

SOURCES AND METHODS OF FOREIGN NATIONALS ENGAGED IN ECONOMIC AND MILITARY ESPIONAGE

THURSDAY, SEPTEMBER 15, 2005

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON IMMIGRATION,
BORDER SECURITY, AND CLAIMS,
COMMITTEE ON THE JUDICIARY,
Washington, DC.

The Subcommittee met, pursuant to notice, at 2:26 p.m., in Room 2141, Rayburn House Office Building, the Honorable John Hostettler (Chairman of the Subcommittee) presiding.

Mr. HOSTETTLER. The Subcommittee will come to order.

We pride ourselves on being an open society in America. We allow millions of foreign nationals to come to our shores each year as tourists, business visitors, and students. Unfortunately, some of these business visitors have come here to take advantage of our openness and engage in economic and military espionage.

Earlier this morning in a closed session, the Subcommittee heard a disturbing report given by the Nation's top counterintelligence official regarding economic and military espionage by foreign nationals in the United States. We will shortly hear a sanitized version of this testimony.

In the past few months alone: American University researcher and Chinese national Zhan Gao pled guilty to illegally exporting technology that can be used in missile guidance and airborne battle management systems for a $590,000 payment from China. Chinese nationals, Jian Guo-qu and Ruo Ling Wang, were arrested in Milwaukee for conspiring to illegally export more than $500,000 in restricted electronic military radar components to China. Iranian Abbas Tavakolian was sentenced to 57 months incarceration for attempting to export F–4 and F–14 jet parts to Iran. Kwonhwan Park, a Korean national, pled guilty in November to illegally exporting Black Hawk helicopter engines to China through a Malaysian front company.

Month after month, publications such as TIME magazine and the Washington Times have run stories concerning the theft of critical American technologies by foreign nationals embedded at research facilities.

Nationals of many nations come to the United States to engage in espionage. Our closest allies are not excluded from this list. However, all evidence indicates that certain nations are the most egregious violators.

There is no nation that engages in surreptitious illegal technology acquisition for purposes of both commercial piracy and military advancement on a scale that approaches that of the People's Republic of China.

The Wall Street Journal reported last month that thousands of Chinese military front companies are operating in the United States—some as contractors for the United States military—and that hundreds of thousands of Chinese tourists, business executives and students entered the United States last year.

Many of these visitors, even when they are visiting for legitimate purposes, are tasked with obtaining whatever technological information they can.

There are currently at least 115 students here from China, studying nuclear engineering, and thousands more studying computer, electrical, civil and chemical engineering. As an engineer myself, I must ask how can we be sure that they are not bringing back American technological secrets to their home country?

And what about Iran, a country we suspect of endeavoring to make nuclear weapons? There are now at least four Iranian nationals actively studying nuclear engineering in the U.S., according to the Department of Homeland Security, as well as 350 electrical engineers, 12 biochemists and a host of other Iranian students studying in technical fields here.

What is true of all these individuals is that they came to the United States after being approved for visas. They undergo Visa Mantis security checks which are designed to weed out those visa applicants likely to use these visits to the U.S. to acquire sensitive technology.

However, the State Department's focus over the last several years seems to have been devoted to reducing the inconvenience of the Visa Mantis security checks for visa applicants as much as possible and to be as generous as possible in the issuance of multiple-entry visas.

Now, we all want to facilitate the swift issuance of visas to legitimate applicants. But, I am concerned that we might not be paying adequate attention to the inherent security risks, that we may be being generous to a fault. At jeopardy are our military superiority and our economic competitiveness.

Today we will ask a number of questions including: what can be done to enhance the existing security systems in place to track foreign nationals at our research facilities? Do background checks for visa applicants need to be improved? And should aliens suspected of being involved with piracy or illegal technology transfer be automatically ineligible for a visa to the United States?

At this time I turn to my colleague, the Ranking Member from Texas, Ms. Jackson Lee, for purposes of making an opening statement.

Ms. JACKSON LEE. Thank you very much, Mr. Chairman, I want first of all to associate myself with the intent of this hearing and what I believe the Chairman's intent is and, of course, associating myself and joining him with that intent, the purpose of this hearing. That would be the legislative road map, the guidepost, if you will, to help us effectively become the America that we all know and have come to love; a country that respects both the invest-

ment—both investment and, of course, the contributions that immigrants have made over the long history of this Nation.

I have always begun these hearings over the last year that I have had the honor of serving my colleagues and the American people, saying that we are a nation of immigrants and a nation of laws, and of course, that immigrants do not equate to terrorists.

So as we look to the witnesses who are before us, let me ask you to keep in mind that it would be, I believe, an impractical nonreality to suggest that we would close the door to all students, all researchers, and all nationals, international persons attempting to do business in the United States.

The subject of this hearing is foreign nationals engaged in economic and military espionage. According to the National Counterintelligence Executive report to the Congress this year, individuals from almost 100 countries attempted to acquire sensitive United States technologies in fiscal year 2004.

The report concludes that foreign access to sensitive information with both military and conventional applications has eroded the United States military advantage and the greater U.S. intelligence community's ability to provide information to policymakers and undercut U.S. industry. It goes to my point that we must separate sort of the weak from whatever else is engaged.

It is interesting that when all of us travel aboard—abroad on behalf of our respective Committees, particularly in this instance, the Homeland Security Committee that I am also on, are also interacting with heads of government who are thanking you for the opportunity of many of their own nationals to engage in training activities and opportunities—and research opportunities with those in the United States.

You will constantly hear from your constituents, mostly in the medical and science professions, technology professions, the importance of the exchange and the ability to interact with those from other countries. This report states, however, that we are vulnerable to espionage because the United States has provided foreign entities with easy access to sophisticated American technologies.

Many people thought that we were on the wrong side of the issue when many of our voices rose to oppose the sale of

Unocal to a Chinese energy company. I happen to be one of those, and I come from what is called the energy capital of the world, but frankly I do believe there should be a fire wall in terms of important technology—and had the opportunity to speak to the head of China's petroleum company at the time that the sale was being pulled, if you will, and indicated that we hope we have the opportunity to do other business efforts with that company, but there had to be a line in the sand on important technologies.

New electronic devices have vastly simplified the illegal retrieval of storage information, of massive amounts of information, including trade secrets and proprietary data. Globalization has mixed foreign and American companies in ways that have made it difficult to protect the technologies that these firms develop or acquire, particularly when that technology is required for overseas operation.

Mr. Chairman, I just a few days ago took my son back to college, interacted with a few college students for a couple of hours, not a whole day, but I was amazed with the level of sophistication and

the eagerness to come back and use either the school's technology or their own to develop new expertise—maybe something like what Bill Gates did a decade or more ago—dealing with now the new Microsoft, this new technology called Facebook, which the college students themselves designed.

We know technologies are being fostered all over America, and the simplicity of being able to access some of our most delicate information is something we should be concerned about.

Lastly, sophisticated information systems that transmit—store and transmit systems have become increasingly vulnerable to cyber attacks, an issue that my colleague Congresswoman Lofgren has been a leading force on. Apparently, the counterintelligence community is uncertain about exactly how much of its intelligence collection effort—some intelligence collection effort is directed by foreign governments and how much is carried out by private businessmen and women, academics or scientists, for purely commercial or scientific purposes.

It is clear, however, that some foreign governments do employ state actors. This includes their intelligence services as well as commercial enterprises.

Most of the foreign governments that are attempting to acquire American technology employ tools and techniques which are easy to use, inexpensive, low risk and sometimes legal. In most cases, foreign collectors simply ask for the information by e-mail, a phone call, a fax, a letter or in person. The report asserts further that increased demand for foreign labor in the United States, high-tech industries and the sharp rise in foreign investment in the United States over the past decade have given foreign governments increased access to American businesses and consequently to U.S. trade secrets.

In addition, recognizing neutral benefits of an unhindered exchange of information, the United States has opened its military bases, national laboratories and private defense suppliers to foreign visitors.

Mr. Chairman, I am going to ask that the entirety of this statement be submitted as I come to a close, and I ask unanimous consent that the rest of my statement be submitted into the record.

Mr. HOSTETTLER. Without objection.

Ms. JACKSON LEE. But let me conclude by saying, we know the problems, but we also know the value and the benefits that have been received by the American people that have been our longstanding commitment and our values to the opportunity of bringing those who are persecuted to the shores, but also those who have talent, who are contributors and those who just have brawn, who have literally built America.

Let us not close the door to the opportunity of foreign students who—again, as I met with in meetings in China and elsewhere, who have learned both our democratic principles but also to share in technology and the ability to build systems that will benefit not China, not Germany, not the new Iraq, not South and Central America or the continent of Africa, but humanity. Let us not in our effort to avoid the transmittal of important technologies and important concepts here in America, not draw technology—draw legislation so restrictive, Mr. Chairman, that we cannot find a way to en-

sure that America benefits from the talent of this world. And let us make sure that the legislation is reflective of the security needs, but also the needs of the American people to be a friend to the world. And I yield back.

Mr. HOSTETTLER. I thank the gentlelady.

Do any other Members have opening statements?

Ms. LOFGREN. Mr. Chairman, I will not take the full 5 minutes.

Mr. HOSTETTLER. I recognize the gentlelady from California.

Ms. LOFGREN. Clearly, every Member of Congress is interested, concerned and opposed to espionage in our country. So that is a given. The question is how to protect ourselves without doing damage to ourselves, and I think it is important to recall. I was in elementary school in 1957 when Sputnik went up, and we got a little wake-up call that the country was in trouble and we were in a huge competition with the Soviet Union, and we were behind. We pulled up our socks, and we ultimately won that competition.

I think in a way we are in a similar spot today, the American Electronic Association used this phrase: It is the difference between then, which was throwing the frog in the boiling water; now the frog is in the water as it heats up, and a lot of Americans don't realize that we are in this competition that is very serious in terms of science and technology and engineering talent. We have slipped in the number of engineering Ph.D.'s awarded in this country. We are falling behind; India and China and the EU are emerging as ever more vibrant competitors.

The AEA—again, they just did a terrific report—cite the U.S. graduating 60,000 engineers a year, India graduating 82,000 engineers a year, and China graduating four times as many engineers a year as the United States.

Now, the Ph.D. level—the National Academy of Sciences tells us that 65 percent of the Ph.D. candidates in engineering are foreign students, and many of them stay on and become Americans with us, and that benefits us greatly. In fact, I come from Silicon Valley, and about 40 percent of the start-ups in Silicon Valley are from people who were born someplace else and became Americans.

And so we need to keep in mind that if we have to have strength in systems to make sure that we are protected, that we don't end up shooting ourselves in the foot economically, and I would say also militarily, because the new Americans, the best and brightest, also help immensely in terms of the technology that ultimately is used, not just in the commercial world, but also in the defense effort.

I hope that as we talk further about this, we can think about what systems we might put in place, smart systems, so that rather than creating bulky systems that have the result of deterring people we might want to have come in, and maybe not deterring the bad guys, we come up with streamlined systems that really target what we need in a way that is efficient and does not do damage.

So that is what I am very interested in, and I yield back the balance of my time.

Mr. HOSTETTLER. I thank the gentlelady.

Without objection, all Members will have—will be allowed to have their opening statements be made a part of the record.

Mr. HOSTETTLER. At this time, I would like to introduce Members of our panel.

Michelle Van Cleave is the National Counterintelligence Executive and, as such, she is the country's top counterintelligence official and is charged with integrating and providing strategic guidance for counterintelligence activities across Government. She reports directly to the Director of National Intelligence, John Negroponte, the President's principal intelligence advisor.

In the 105th Congress, Ms. Van Cleave was Chief Counsel for the Senate Judiciary Subcommittee on Technology, Terrorism and Government Information.

In 1989, she served on the House Science Committee staff and was later Assistant Director in the White House Office of Science and Technology Policy. She has also held senior positions at the Department of Defense and is a graduate of the University of Southern California Law School.

Dr. Larry Wortzel has been at the Heritage Foundation since 1989 and has served as Asia Studies Director. He is a former Marine, Army Airborne Ranger and Army Colonel, and has worked for the Under Secretary of Defense for Policy to develop counterintelligence programs. In 1970, he served in the U.S. Army intercepting Chinese military communications in Vietnam and Laos. Later, his career took him to areas throughout Asia under U.S. Pacific Command and as U.S. Army Attache at U.S. Embassy Beijing during the Tiananmen massacre, and in 1995.

Dr. Wortzel is the author of numerous books on Chinese military strategy and received his Ph.D. at the University of Hawaii.

Mr. Maynard Anderson is President of Arcadia Group Worldwide, Incorporated. He has served in Government as Deputy Under Secretary of Defense for Security Policy with the responsibility of setting disclosure policy. In 1988, he served as Assistant Deputy Under Secretary of Counterintelligence of the Department of Defense, setting security policy and providing day-to-day oversight.

Mr. Anderson also chaired the National Foreign Disclosure Policy Committee. Privately, he served as Chairman of the National Intellectual Property Law Institute Board of Directors. Mr. Anderson is a graduate of Luther College in Iowa and the Federal Executive Institute.

William Wulf is President of the National Academy of Engineering and Vice Chair of the National Research Council. He is on leave from the University of Virginia, where he is AT&T Professor of Engineering and Applied Sciences. Mr. Wulf has served as Assistant Director of the National Science Foundation and Chief Executive Director of Tartan Laboratories, Inc., in Pittsburgh. He was also a Professor of Science at Carnegie Mellon University. He has authored more than 100 technical reports, has written three books and holds two U.S. patents.

At this time, will the witnesses please rise to take the oath.

[Witnesses sworn.]

Mr. HOSTETTLER. Thank you. You may be seated. Please let the record show that each of the witnesses answered in the affirmative.

Ms. Van Cleave, you are recognized for purposes of an opening statement.

TESTIMONY OF THE HONORABLE MICHELLE VAN CLEAVE, NATIONAL COUNTERINTELLIGENCE EXECUTIVE, OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

Ms. VAN CLEAVE. Thank you, Mr. Chairman. I do have a prepared statement I would like to submit for the record.

Mr. HOSTETTLER. Without objection.

Ms. VAN CLEAVE. Please let me summarize a few points.

I appreciate very much the opportunity to appear before you today to discuss foreign intelligence threats to U.S. national intelligence security and our economic well-being.

Since some of the Members of the Subcommittee may not be familiar with my office, I would like to take a moment to describe my duties. In the post-Cold War world, the U.S. confronts intelligence challenges from a broad array of foreign nations. The singular global Soviet threat of decades gone by has been succeeded by a diverse set of adversaries, many of whom have become highly skilled in using their intelligence services, especially their human collectors, to acquire U.S. national security secrets. These include the technological and engineering secrets that give our Armed Forces the qualitative edge they may need to prevail in a dangerous world.

While the threats against us are strategic, historically the U.S. counterintelligence community has not been organized or integrated to accomplish a national strategic mission. On the contrary, the various counterintelligence elements have long been part of a loose confederation of independent organizations with different jurisdictions and capabilities and no one in charge of the enterprise.

CI operations and investigations have tended to focus on individual cases with little appreciation of synergy or their larger strategic implications. This structural flaw has undercut our ability to connect the dots of intelligence anomalies or effectively coordinate the different CI arms of our Government. To help remedy this situation, the Congress created the position of the National Counterintelligence Executive, or the NCIX. The law directs that the NCIX shall serve as the head of counterintelligence for the U.S. Government, subject to the direction and control of the Director of National Intelligence.

I am the first NCIX appointed by the President. It is my job to provide strategic direction to our Nation's counterintelligence efforts and to assure the integration of the disparate CI activities of our Government. It also includes the counterintelligence dimension to broad national security concerns such as the protection of our Nation's critical technologies.

The primary focus of counterintelligence is to defeat the efforts of foreign intelligence services to acquire U.S. national security secrets. It is also our job to supply CI insights and options to the President and his national security leadership. This includes supporting the overall national effort to stem the outflow of sensitive technologies, including export controls, diplomatic measures, controls on foreign investments in sensitive sectors of the U.S. economy and industrial security agreements.

I want to emphasize that by far the vast majority of foreign acquisition of U.S. technology is open and lawful, as are the transactions of individuals and businesses involved in international com-

merce, as well as the free exchange of ideas in scientific and academic forums. But let me turn to the cases that fall outside the bounds of what is open and lawful.

Last year, the counterintelligence community tracked efforts by foreign businessmen, scientists, academics, students and government entities from almost 100 countries to acquire sensitive U.S. technologies protected by export laws or other means. Of those, the top 10 countries accounted for about 60 percent of the suspicious foreign collection efforts against cleared defense contractors. Two of the countries that always rank near the top of the list are, of course, Russia and China, who have particularized interests, especially in dual-use technologies with military applications.

But the top 10 also include some of our close allies, as you noted, Mr. Chairman. These allies may exploit their easy access to push the envelope into areas where they have not been invited.

In the majority of cases, foreign collectors simply ask. By e-mail or phone calls or faxes or letters or in person they ask for the information or technology that they are interested in. Or they may exploit visits to U.S. businesses or military bases, national laboratories and private defense suppliers to extract protected information.

U.S. businessmen and scientists and academics traveling abroad provide another valuable source of information for foreign countries, as do foreign students, scientists and other experts who to come to the U.S. to work or attend conferences.

One indirect method used to acquire technology is for foreign firms to offer their services or technology, particularly IT-related support, to firms who have access to sensitive items.

On this point, I should note that the use of cyber tools, as a collection technique, is of growing concern. As you know, cyber exploitation is inherently difficult to detect, as cyber intruders from one country will typically cover their tracks by mounting their attacks through compromised computers in other countries.

Finally, state-directed espionage: State-directed espionage remains the central threat to our most sensitive national security technology secrets.

While the Chinese, for example, are very aggressive in business and good at solicitation and good at positioning themselves for strategic investments, and they are adept at exploiting front companies, they also have very capable intelligence services that target U.S. national security secrets. As the Cox Commission report made clear over a decade ago, the Chinese did not acquire the most sensitive secret U.S. nuclear weapons designs by spending late nights at the library.

It is one thing to describe these threats to you; it is quite another to describe what we need to do about them. We will never have leak-proof technology controls, just as we will never have enough security to protect us against all the threats all the time. Nor would we want to exchange the vast blessings of our free society for a security state.

In my view, good security is not the answer alone. We also must have good counterintelligence, meaning that we must be more proactive in identifying, assessing and degrading foreign intelligence operations against us. We need to prioritize our efforts

against the most serious threats to U.S. national security and our vital defense and foreign policy objectives.

Now, in March of this year, President Bush approved the first national counterintelligence strategy of the United States, which I would like to submit for the record, if I may, Mr. Chairman.

Mr. HOSTETTLER. Without objection.

Ms. VAN CLEAVE. It is the first mission statement of counterintelligence as an instrument of U.S. national security policy. This is a very different concept of counterintelligence than the common perception of catching spies and putting them in jail. Counterintelligence encompasses all activities to identify, assess and degrade foreign intelligence threats to U.S. national security and our foreign policy objectives. And central to the President's strategy is the call for U.S. counterintelligence to be proactive.

Now, this Committee has jurisdiction over America's single greatest resource for encountering intelligence threats, the Federal Bureau of Investigation. In the months to come, the FBI will be standing up a new national security branch that will span its responsibilities for counterterrorism, intelligence, and counterintelligence.

Building on Director Mueller's efforts to date, the full integration of these disciplines should enable the FBI to recruit, train and develop a new generation of agents and support personnel dedicated to its core national security mission. And more complete integration of the FBI with sister counterintelligence agencies will augment our nation's ability to protect against the most serious foreign intelligence threats.

In closing, Mr. Chairman, I would like to thank you very much for this timely hearing, and I welcome your questions.

Mr. HOSTETTLER. Thank you, Ms. Van Cleave.

[The prepared statement of Ms. Van Cleave follows:]

PREPARED STATEMENT OF THE HONORABLE MICHELLE VAN CLEAVE

UNCLASSIFIED

STATEMENT FOR THE RECORD
National Counterintelligence Executive
The Honorable Michelle Van Cleave
before the
House Judiciary Subcommittee on Immigration, Border Security & Claims

Hearing on Sources and Methods of Foreign Nationals
Engaged in Economic and Military Espionage
September 15, 2005

Mr. Chairman and members of the committee, thank you for the opportunity to testify today on the subject of foreign intelligence threats to America's vital military and other sensitive technologies.

Let me begin by telling you a little about my office, the National Counterintelligence Executive (NCIX), which was created in the wake of a series of debilitating spy scandals that rocked our nation over the past decade and a half. You will no doubt remember Aldrich Ames, a former CIA counterintelligence (CI) officer, who was arrested in 1994. He spied for the Russians for nearly a decade, during which period some 30 operations against the Soviets were compromised, and at least 10 Russians and East Europeans were executed as a result of his espionage. Indeed, as the Senate Intelligence Committee reported, Ames was responsible for the loss of virtually all of CIA's human intelligence assets targeted at the Soviet Union at the height of the Cold War.

At the time, it was believed that Ames was the most damaging spy in U.S. history, but, in fact, there were others also spying at that time who would vie for that title. FBI Agent Robert Hanssen, arrested in 2001, spent at least 21 years serving the same master as Ames. He compromised sensitive programs and intelligence capabilities that cost the U.S. Government more than $22 billion. Also hard at work for another country, Cuba, was the lesser known, but potentially no less damaging spy, DIA analyst Ana Montes. She spent 17 years betraying our country.

The losses that these and scores of other spies inflicted resulted in grave damage and danger during peacetime; they could have had catastrophic consequences had we found ourselves at war. Now we are at war with terrorists and facing continuing threats from other adversaries, and the potential consequences of intelligence failure are far more immediate, putting in jeopardy deployed forces, ongoing operations, and the lives of troops abroad as well as Americans at home. Indeed, each of the major challenges confronting the nation's security today—defeating global terrorism, countering weapons of mass destruction, ensuring the security of the homeland, transforming defense capabilities, fostering cooperation with other global powers, and promoting global economic growth—has an embedded counterintelligence imperative. We must protect

against those who engage in a range of intelligence activities directed against U.S. interests and objectives at home and abroad.

To counter continuing espionage and other foreign intelligence threats against America's national security secrets, and to deal with these new challenges, the United States requires a national, systematic perspective and coherent policies, including a strategic counterintelligence response. It is for exactly these reasons that the Congress created the position of the NCIX. The CI Enhancement Act of 2002, which established my office, directs that the NCIX head national counterintelligence for the U.S. government, subject to the direction and control of the Director of National Intelligence. As NCIX, I chair the National CI Policy Board, which is the principal mechanism for developing policies and procedures for the approval of the President to govern the conduct of CI activities. I also lead a 64-person Office of the National Counterintelligence Executive (ONCIX), which is now within the office of the DNI.

ONCIX has the core mission of providing strategic direction to the nation's counterintelligence efforts overall. Specifically my office is responsible for:

- Developing the National CI strategy, an unprecedented effort in the annals of U.S. counterintelligence.
- Providing annual assessments of the foreign intelligence capabilities of our adversaries and the threat they pose to the United States.
- Overseeing and coordinating strategic analyses on critical CI issues, as the threat, technology, and our interests and vulnerabilities continue to evolve.
- Drafting assessments to gauge and help remediate the damage inflicted by the spies we have caught, such as Ames, Hanssen and Montes.
- Developing and setting priorities for CI collection requirements across the Community.
- Developing policies and standards for training and educating CI professionals in the challenging art and tradecraft of CI.
- Fostering heightened public awareness of basic CI threats to our nation.
- Providing budget guidance for the CI Community to ensure that the nation's resources are focused on the key CI tasks outlined in the National CI Strategy.

Nearly 140 nations and some 35 known and suspected terrorist organizations currently target the United States for intelligence collection through human espionage and by other means. Their purposes are many: to steal our national security secrets to support their war aims or terrorist objectives, or to undercut us in foreign policy or commerce, or to exploit what they learn of our intelligence capabilities to hide their actions or mislead us. If left unanswered, their success could come at dear cost, putting in jeopardy U.S. operations, military and intelligence personnel, and Americans at home.

Effective counterintelligence is a strategic imperative to protect American lives and operations and to support the advance of freedom.

In March of this year, the President approved the nation's first National CI Strategy, which I would like to submit for the record. Its purpose is to direct and unify U.S. counterintelligence activities to achieve strategic objectives in support of the nation's security. The Strategy speaks directly to the critical issues that are before this Committee today: protecting critical U.S. technologies, trade secrets, and sensitive financial or proprietary economic information from foreign collectors.

The foreign theft of sensitive dual-use and military technologies has eroded the U.S. military advantage by making dangerous technology available to our adversaries. In addition, it has degraded the U.S. Intelligence Community's ability to provide information to policymakers, and it has undercut the competitiveness of U.S. industry by allowing foreign firms to acquire, at little or no cost, technology that U.S. firms spent hundreds of millions of dollars developing.

Stopping the illicit foreign acquisition of sensitive U.S. technologies must be addressed through a combination of national security tools: export control laws, diplomatic measures, industrial security arrangements, limits on foreign investment in strategic U.S. industries, and counterintelligence.

It is the job of U.S. counterintelligence to identify the foreign intelligence hand orchestrating efforts to acquire sensitive U.S. technologies. The primary focus of CI is to defeat the efforts of foreign intelligence services to acquire U.S. national security secrets. It is also our job to support larger national policy efforts to stem the outflow of sensitive technologies. My office was created, in part, to contribute this essential CI policy piece to our nation's national security and homeland security objectives.

Sensitive U.S. technologies—those that both underpin the U.S. economy and contribute to U.S. military prowess—remain prime targets for foreign acquisition, both lawful and illegal. To this end, foreign companies, scientists, academics, and others see the acquisition of U.S. technology as key to advancing their economic and military interests.

A World of Increased Foreign Access to Sensitive U.S. Technology and Trade Secrets

The globalization of the U.S. economy and the explosive growth in technology, especially information technology (IT), have been double-edged swords. Some of the very factors that have significantly contributed to U.S. economic growth and technological progress have at the same time facilitated foreign entities' technology acquisition efforts against us. For example:

- Our general culture of openness has provided foreign entities easy access to sophisticated technologies. Each year, for example, we allow tens of thousands of official foreign visitors into U.S. Government-related facilities such as military bases, test centers, and research laboratories. Some of these visitors are dedicated to acquiring U.S. technology and know-how not otherwise available.

- American colleges and universities, centers for high-tech development, employ large numbers of foreign born faculty and train large numbers of foreign students, many of whom will return to their home countries. For example, an increasing number and share (approaching 30 percent) of science and engineering faculty employed at U.S. universities and colleges are foreign born, according to National Science Foundation statistics. Moreover, the most recent data available indicate that about 40 percent of the PhDs awarded by U.S. universities in technical sciences and engineering—roughly 8,000 per year—now go to foreign students. The vast majority of these students are legitimately studying and advancing academic pursuits. But some are not.

- Breathtaking advances in IT have vastly simplified the illegal retrieval, storage, and transportation of massive amounts of information, including trade secrets and proprietary data. Compact storage devices the size of a finger and cell phones with digital photographic capability are some of the latest weapons in technology transfer as are the tools of cyberspace.

- Sophisticated information systems that create, store, process, and transmit sensitive information have become increasingly vulnerable to cyber exploitation. Many nations have formal programs for gathering our networked information, and foreign competitors are developing the capability to exploit those vulnerabilities.

- Globalization has mixed foreign and U.S. companies in ways that have made it difficult to protect the technologies these firms develop or acquire, particularly when that technology is required for operations overseas. In 2004 alone, according to the Department of Commerce, foreign investment in the United States amounted to more than $100 billion. A couple of the notable foreign acquisitions of U.S. high-tech companies in the past few years include the purchase of fiber optic network provider Global Crossing by Singapore Technologies and the more recent takeover of IBM's personal computer business by China's computer giant Lenovo.

The Major Threats

Given the access that foreigners have to U.S. technology and the importance of that technology to their economic and military development, it should be no surprise that individuals from many countries are involved in the creative acquisition of U.S. technology including theft. In FY2004 alone, the CI Community tracked efforts by foreign businessmen, scientists, academics, students, and government entities from almost 100 countries to acquire sensitive U.S. technologies.

In order to discuss in detail the specific countries involved in this technology transfer, we would need to go into closed session, but a couple of points about the collectors are notable. First, while the number of countries seems large, in fact, most of the activity was conducted by individuals from a very few locations. The top 10 collectors, for example, probably accounted for 60 percent or so of the suspicious foreign collection efforts against U.S. cleared defense contractors last year, according to reporting from the Defense Security Service. The countries in

that top-10 list are a diverse group. They include some of our closest allies as well as some of our adversaries. Among them are countries where per capita income levels are high as well as those at the other end of the scale. Two countries that always rank near the top of the list and that are frequently cited in the press are, of course, China and Russia.

It is difficult to determine how much of the theft of U.S. sensitive technology is being directed by foreign governments and how much is simply being carried out by private businessmen, academics, or scientists for purely commercial or scientific reasons. Importantly, in many cases we do not know how much of a nexus there is between the private and public sectors that are targeting our technologies. Anecdotal evidence and incomplete statistical information indicate that much trade secret and technology theft takes place without direct intervention by foreign governments, though most foreign governments that are involved do not discourage such theft and themselves often benefit from the transfers. It is clear, however, that the major threat countries continue to employ state organs—including their intelligence services—as well as commercial enterprises, particularly when seeking the most sensitive and difficult to acquire technologies. In addition, we note that a number of countries have begun to establish institutions at home and in the United States to take full advantage of technology acquired by private citizens working or studying here.

The Methods of Operation

We face significant intelligence gaps in understanding how foreign nations collect against U.S. technology. But there are a number of things the CI Community can say with confidence about the perennially serious problem of state-sponsored industrial espionage. For example, we know that a number of the major foreign intelligence agencies have:

- Dedicated programs whose primary task is technology acquisition. These programs often involve the use of front companies, which operate surreptitiously.

- "Laundry lists" of targeted technologies and specific strategies for acquisition. Where an entire system cannot be acquired, foreign intelligence services may attempt to steal component parts.

- Arrangements to share technology that has been both legally and illegally acquired with other countries' intelligence and security services, even when the sharing of that technology is itself illegal.

Overall, the techniques used to acquire sensitive U.S. technologies are far broader than those traditionally associated with espionage. In the case of China, for example, its national-level intelligence services employ a full range of collection methodologies, from the targeting of well-placed foreign government officials, senior scientists, and businessmen to the exploitation of academic activities, student populations, and private businesses. The Chinese intelligence efforts take advantage of our open economic system to advance China's technical modernization, reduce the U.S. military advantage, and undermine our economic competitiveness. Let me highlight for

you some of the relatively new methods that China and other state and non-state collectors sometimes use to gain access to our technology. As might be expected, the techniques that are easiest to use, least expensive, and lowest risk are the ones first and most often employed.

For example, **in a majority of cases, foreign collectors simply ask—via e-mail, phone call, FAX, letter, or in person—for the information or technology.** When a foreign request for U.S. technology is either refused by a U.S. company or the U.S. firm asks the foreign firm to apply for an export license, the foreign company often simply breaks off communication and looks for another possible U.S. seller. With search costs extremely low, the foreign firm can afford to continue looking until it locates a U.S. company that either does not understand the export licensing requirements or is willing to ignore them in order to make the sale.

Another common technique employed by foreign entities is to exploit visits to U.S. businesses, military bases, national laboratories, and private defense suppliers. Recognizing the mutual benefits of an unhindered exchange of information, the United States opens its military bases, national laboratories and private defense suppliers to foreign visitors. Even foreign students and academics visiting U.S. universities where high-tech experiments are underway can present problems. The CI Community receives incident reports about foreign experts wandering into restricted areas, peppering U.S. researchers or scientists with questions well outside the range of issues they are supposed to discuss, and taking photographs of sensitive equipment that the foreign experts are not supposed to see.

The losses that result from such visits can be significant. Such foreign visitors are often among their nations' leading experts and, as such, may be much more effective at extracting sensitive information than would be traditional foreign intelligence officers. Specialists know their countries' or companies' specific technological gaps and can focus their collection efforts directly on the critical missing information. Finally, such experts are also in a position to recognize and exploit information that may be inadvertently exposed during visits.

And the technology losses to long-term foreign visitors can be even more significant than those to foreign experts making shorter visits. For one thing, overseas specialists who stay on site for extended periods of time become familiar with, and learn to circumvent, the security procedures meant to limit their access to sensitive technologies. This is particularly true of cyber security procedures. A long-term presence may allow visitors time to acquire passwords and to learn where on hard drives sensitive information is stored. Whereas short-term visitors are viewed as strangers on sensitive sites, long-term visitors become part of the landscape. Their activities naturally receive less notice, which enables them to wander into sensitive areas without attracting undue attention.

Increasingly the CI Community is most concerned about cyber tools being used in efforts to extract sensitive information. The insider threat—an individual with access to a U.S. firm's computer system but actually working for a foreign entity—is, of course, of most concern. But the Community is also worried about other cyber exploitation techniques, including probing, scanning, phishing, spamming, virus dissemination and the use of sophisticated hacking tools,

many of which are available online. Cyber exploitation is inherently difficult to detect as cyber intruders from one country typically cover their tracks by routing their attacks through the compromised computers of others. At the same time, the losses can be significant and finding the cyber bandit can be virtually impossible.

U.S. businessmen traveling abroad provide another valuable source of information for foreign countries. Foreign governments and businesses continue to acquire sensitive U.S. proprietary information from all types of electronic storage devices, including laptop computers, personal digital assistants (PDAs), and cell phones carried by U.S. businessmen traveling abroad. A recent U.S. private sector study indicated that two-thirds of PDAs are used to carry client details and corporate information but without adequate protection. Foreign businesses and security services gain access to such information by using clandestine entry to hotels and business establishments or by electronically downloading information during routine security inspections at airports or other ports of entry. In addition, technology weaknesses in some PDAs make it easy for foreign entities to extract information without directly accessing the storage devices.

Foreign students, scientists, and other experts who come to the United States to work or attend conferences also can serve as a funnel for sensitive U.S. technologies. China, in particular, seems to be benefiting from the access its experts have here. The Chinese press explicitly recognizes the role of the overseas Chinese community in increasing China's technological prowess. Moreover, Beijing has established a number of outreach organizations in China and it maintains close relations with a number of U.S.-based advocacy groups that facilitate its interaction with experts here and probably aid in efforts to acquire U.S. technology.

One indirect method used to acquire U.S. technology is for foreign firms to offer their services or technology—particularly IT-related support—to U.S. firms that have access to sensitive items. Such deals, at a minimum, have provided foreign visitors access to facilities where trade secrets or proprietary information are stored. In their most dangerous forms, however, these deals can result in foreign companies subverting U.S. firms' supply chains by selling tainted products. These subversions could give foreign companies long-term, remote access to significant proprietary information and trade secrets. Well-executed supply chain subversions are almost impossible to detect, even years after implantation.

In some cases, foreign entities seeking to acquire sensitive U.S. technologies find that the easiest route to acquisition is to **either purchase outright or form a joint venture with a U.S. firm that has access to that technology.** Even joint venture negotiations where no agreement is reached can yield proprietary information valuable to foreign entities. The negotiation process often includes plant tours and inspections of manufacturing processes, and the U.S. firms may provide proprietary information on customers and marketing plans in an effort to secure the deal.

Increasingly, foreign entities need not even come to the United States to acquire sensitive technology but, instead, can work within their own borders. There, U.S. firms have difficulty securing their secrets and have few legal protections once proprietary information has

been lost. Globalization is forcing U.S. companies toward a more diversified business model that includes foreign outsourcing and external partnerships. These arrangements, while making U.S. firms more competitive by providing a source of inexpensive inputs, at the same time make sensitive U.S. technologies more vulnerable. For example, a recent security survey by a major U.S. accounting firm showed that sensitive blueprints, formulas, and computer codes are being transferred abroad to enable foreign firms to supply specially tailored inputs to high-tech products that are manufactured in the United States.

Conducting due diligence on foreign partners is difficult, but the problem becomes geometrically more complicated when the foreign partners themselves outsource to other firms. According to the same security survey just cited, fewer than one-third of U.S. companies that are involved in outsourcing conduct regular assessments of their IT providers to monitor compliance with information security policies; "they simply rely on trust." These trends not only leave U.S. firms more exposed to a direct outflow of technology but also make it difficult to guarantee that the foreign-provided inputs—particularly IT hardware and software—are free from Trojan horses or back doors that could be used later to extract sensitive technology.

The Technologies Targeted

What kinds of technologies are targeted? Virtually all kinds of U.S. trade secrets—military and civilian—are targeted. The CI Community pays closest attention to technologies with direct military application and to those on the Defense Department's Militarily Critical Technologies List (MCTL), many of which are dual-use, with both military and commercial applications. All of the technologies on the MCTL are targeted every year. **Information systems**—the foundation of almost all modern civilian and military production processes—continue to top the list of targeted technologies. There has also been significant foreign interest in **sensors**, which provide the eyes and ears of many military systems; **aeronautics**, because of the demonstrated advantage of airpower in recent international conflicts; **electronics**, which are either contained or used in the production of virtually every weapons system in the U.S. arsenal; and **armaments and energetic materials**, the technologies required to develop and produce conventional munitions and weapons systems of superior operational capability.

As difficult as it is for us to track foreign efforts to acquire military and dual-use technologies—where defense contractors are required to report suspicious targeting incidents—it is far more challenging for the CI Community to monitor foreign targeting of purely commercial technologies. The FBI has outreach programs that are geared to encouraging U.S. firms to report suspicious targeting incidents but, even so, such reporting is uneven at best. U.S. firms have sometimes been reluctant to raise alarms about possible technology theft out of concern for the potential impact on investor and consumer confidence and stock prices. Nevertheless, recent legal cases alleging technology theft provide examples of the items targeted, which include: semiconductor production processes, computer microprocessors, high-speed digital cameras, software, proprietary information, and chemical formulas.

The Rough Road Ahead

We should expect no decline in foreign demand for sensitive U.S. technologies over the next few years. The United States remains the source of much of the world's most advanced technology, and, in many industries, foreign entities depend on that innovation to improve their competitiveness. At the same time, the task of slowing the illicit outflow of technology will only become more difficult. Globalization, while benefiting the United States economically, is making it challenging to isolate trade secrets from foreign managers and employees. Increasingly U.S. firms are conducting research and development in centers located outside U.S. borders, where physical security will be difficult to maintain and legal protection of technology, trade secrets, and innovation is weak or nonexistent. At the same time, however, U.S. businesses prefer to operate in an environment where their trade secrets are protected, which may gradually pressure foreign governments to strengthen legal safeguards.

It is one thing to list the range of foreign technology acquisition activities to you; it is quite another to describe what we need to do about them.

In my view, successful policy must be consistent, and thoughtfully apply the full range of public policy instruments to strategic effect. For its part, U.S. counterintelligence has to be more effective than the foreign intelligence services—meaning more pro-active in identifying, assessing and degrading foreign intelligence operations against us.

My office has underway an aggressive program to identify, align and coordinate the many CI community efforts to slow this illicit outflow of U.S. technology. We are grouping these activities as the centerpiece of our implementation planning for the National CI Strategy and the recommendations of the Silberman-Robb Commission. Major efforts include, for example, the work of the FBI-led national CI working group on technology protection and a number of cyber threat and technology vulnerability response initiatives.

Mr. Chairman, your Committee has jurisdiction over our nation's single greatest resource in countering foreign intelligence threats, the Federal Bureau of Investigation. The most significant change of late, and it is significant indeed, is the President's June decision to create a new National Security Bureau within the FBI. The integration of counterterrorism, counterintelligence, and intelligence programs in the new NSB should give a major boost to our nation's CI capability, and to achieving the objectives of the National Counterintelligence Strategy.

Mr. HOSTETTLER. Dr. Wortzel.

TESTIMONY OF DR. LARRY WORTZEL, VISITING FELLOW, THE HERITAGE FOUNDATION

Mr. WORTZEL. Mr. Chairman, Members of the Committee, thank you for the opportunity to testify today on the theft of national security secrets and national security sensitive technology. I have a longer statement I would like to submit for the record, if I may.

Mr. HOSTETTLER. Without objection.

Mr. WORTZEL. I will focus on the intelligence collection posed by China. The manpower pool available to the Chinese Government and its intelligence services is nearly limitless, and it is impossible to know for certain if people are here to study for research or if they are here to steal our secrets.

The People's Republic of China is methodical in its program to gather information from abroad. In 1986, the People's Republic of China launched a national high technology research and development program with the specific goal of benefiting China's medium and long-term high technology development.

This is a centralized program; it is known as the 863 Program for the date it was announced, and it allocates money to experts in China to acquire and develop things like biotechnology, space technology, laser technology, and advanced materials. Thousands of Chinese students and scientists were sent abroad by China over the years to pursue critical, civil and military dual-use technologies, and the practice still continues. Thus, the U.S. faces an organized program out of China that is designed to gather high technology information of military use.

Now, today, inside China, there are entire high technology incubator zones that are designed to attract back students from the U.S. or U.S. businesses to bring technology in. It is very important to recognize that Chinese diplomatic missions abroad monitor the activities of their businessmen and students to cultivate informants, and before Chinese citizens get passports or travel permission, they are often interviewed by China's intelligence security services and sensitized to intelligence collection requirements.

I think it is important to remember that the constitution of the People's Republic of China characterizes the state as a people's democratic dictatorship. So it is pretty hard for legal travelers to simply turn down the Chinese Government in that authoritarian state when they get asked to cooperate.

Now, we know from Chinese defectors and Chinese security officials, or diplomats in places like Australia and Canada recently, that this approach is used not only to collect intelligence in the United States, but also abroad.

In 2003, the State Department approved some 700,000 visas for visitors from China to the United States. That includes about 135,000 students. That is just a lot of folks. There were 40,000 immigrant visas granted to Chinese citizens in 2003. I have to say that these numbers make it impossible for the Federal Bureau of Investigation to vet every one of these people. There are some 3,200 Chinese front companies operating in the United States.

Now, the People's Liberation Army of China went into the business of starting companies to bring in technology in the 1970's, late

1970's and 1980's. The General Equipment Department started Polytechnologies; the General Political Department, started Kaili or Kerry Corporation, Baoli, the logistics department started Xinshidai, or the New Era Corporation; and these are separate legal entities, not part of the military, but they were authorized to conduct these activities by the Central Military Commission of the Chinese Communist Party.

They were originally manned by former officers of PLA or their families, in some case active officers, and they operated branches in the United States. They regularly brought delegations to the U.S. to bring in technology, and today they have turned into global conglomerates that have spawned some of those 3,200 companies that are operating in our country.

So the Chief of FBI Counterintelligence Operations, David Szady, recently said that these companies are operating in such places as Milwaukee, Trenton, New Jersey, and Palo Alto.

Now, I think that the Government, the U.S. Government security intelligence and law enforcement agencies have to focus on national security information. They ought to be looking for violations in the Arms Export Control Act, or the Export Administration Act, but when it comes to corporate or industrial espionage, proprietary secrets, that is not national security.

It may be an economic problem for the United States, but I think that there the Government owes American companies a good legal infrastructure to protect patents, copyrights and trademarks; a system of education on industrial security here in our country; and a strong effort to ensure that China meets its own obligations to create a rule of law that protects the rights of ownership and intellectual property. But we shouldn't cross over into losing—given the number of people, into losing our focus on national security.

From the standpoint of congressional action, I would point out that the Export Administration Act expired in 2001; it was a 1979 act. It needs to be revised to take account of the needs of 21st century technology. The Senate passed a revision in 2001; the House did not. I think the Executive Branch has to regularly review the Commodity Control List to ensure that appropriate national security controls on exports do not unduly restrict the ability of American industry to compete in the world market.

Generally speaking, I think that technologies that are widely available in the world market and not unique to the United States should not be restricted and subject to export controls unless they can be multilateral controls. I would also recommend that visa officers get educated by the intelligence community so that things like the Visas Mantis program, and the technology alert list, can work effectively. They have a lot of prerogatives when they are out in the embassy.

Let me close by saying that I don't think it pays for us to be paranoid and suspect that every traveler, student and businessman from China, or woman from China, is a spy or is out to steal technology. Prudent law enforcement programs, counterintelligence programs, security education and industrial security programs are important ways to protect our Nation. But I would note that in places like Taiwan, the Republic of China and South Korea, it is these students that came out and learned and went back home that

changed the political system there and created a rule of law and democracy, and that could someday happen in China. In the meantime, I do think we need to be vigilant.

And I thank you for the opportunity to testify today.

Mr. HOSTETTLER. Thank you, Dr. Wortzel.

[The prepared statement of Dr. Wortzel follows:]

PREPARED STATEMENT OF LARRY M. WORTZEL

Mr. Chairman, Members of the Committee,

Thank you for the opportunity to testify today on the theft of national security sensitive technology in the United States. As a former military intelligence officer who has tracked the activities of the People's Liberation Army and Chinese intelligence services for 35 years, I know of no more pervasive and active intelligence threat to America's national security than that posed by the People's Republic of China. The manpower available to the Chinese government and its corporations to devote to gathering information in the United States is nearly limitless. There are some 300,000 visitors to the United States from China each year. It is impossible to know if these people are here for study and research or if there are here to steal our secrets.

In 2003, for example, the State Department granted about 27,000 visas to Chinese "specialty workers," the H1-B visa. Some of these were intra-company transfers coming to the United States from US firms operating in China. Indeed, between 1993 and 2003 there were about 40,000 immigrant visas from China a year. The US government has handled about 2,410 asylum cases from China a year. In 2003, there were about 55,000 student visas granted to Chinese students. The sheer magnitude if these numbers presents a great challenge to the Federal Bureau of Investigation, particularly when the US is also concerned about terrorism.

The General Political Department of the People's Liberation Army has a proprietary company, Kaili, or Kerry Corporation, that operates in the U.S. as a real estate and investment company. The General Equipment Department of the PLA operates a proprietary company, Polytechnologies, which has offices here in the U.S. In addition, the Chinese Defense, Science, Technology and Industry Commission operate a proprietary called Xinshidai, or New Era, that has offices in our nation. These technically are independent legal entities, but they were established by the Central Military Commission of China to serve the interests of the military industrial complex. The PLA regularly operates trade fairs to attract American high technology into China.

The Deputy Undersecretary of Defense for Technology Security and Counterproliferation has testified that there are between 2,000 and 3,000 Chinese front companies operating in the United States to gather secret or proprietary information, much of which is national security technology or information.

The nature of the Chinese state complicates the problem of knowing what the large numbers of travelers and students from China are actually doing. China is still an authoritarian, one-party state led by the Chinese Communist Party with a pervasive intelligence and security apparatus. The Chinese government is able to identify potential collectors of information and, if necessary, to coerce them to carry out missions on behalf of the government because of the lack of civil liberties in China. Let me quote the first three sentences of Chapter 1, Article 1, of the Chinese Constitution: "The People's Republic of China is a socialist state under the people's democratic dictatorship led by the working class and based on the alliance of workers and peasants. The socialist system is the basic system of the People's Republic of China. Disruption of the socialist system by any organization or individual is prohibited."

The People's Republic of China is methodical in its programs to gather information from abroad. In March 1986, the PRC launched a national high technology research and development program with the specific goal of benefiting China's medium and long-term high technology development. This centralized program, known as the "863 Program" for the date when it was announced, allocates money to experts in China to acquire and develop bio-technology, space technology, information technology, laser technology, automoation technology, energy technology and advanced materials. The 863 program was proposed by China's strategic weapons scientists to emphasize strategic civil and military technology development. Thousands of students and scientists were sent abroad by China over the years to pursue critical civil and military, dual-use technologies. This practice still continues. When I was at the American Embassy in China and conducted due diligence checks to confirm the nature of Chinese companies seeking to do high technology business in the

United States I most often found that the address identified for a company on a visa application turned out to be a People's Liberation Army or PRC government defense research institute. Thus, the United States faces an organized program out of China that is designed to gather high technology information of military use.

My colleague today, Mr Maynard Anderson, will discuss some of the ways that our government and industry can defend against intelligence gathering by China through defensive counterintelligence and security education programs. It is also important to know that we have other programs to screen out people coming to the United States to gather our trade or military secrets. In January 1998, the VISAS MANTIS program was developed to assist the American law enforcement and intelligence communities in securing U.S.-produced goods and information that are vulnerable to theft. Travelers are subject to a world-wide name-check and vetting procedure when they apply for visas. The security objectives of this program are to prevent the proliferation of weapons of mass destruction and missile delivery systems; to restrain the development of destabilizing conventional military capabilities in certain regions; to precent the transfer of arms and sensitive dual-use items to terrorists; and to maintain United States advantages in militarily critical technologies. This program operates effectively and can vet a Chinese student in as few as 13 days. Non-students may take longer, as many as 56 days. However, I can tell you based on my trip to China two weeks ago that the American Embassy in Beijing and the Consulate in Guanzhou are able to process and vet in about two weeks visas for non-student travelers who fully and accurately outline the purpose and itinerary of their trip. The government also operates a "technology alert list" to identify legal travelers from China that may benefit from exposure to advanced U.S. technology with military application.

Many provinces and municipalities in China now operate high technology zones and "incubator parks" specifically designed to attract back Chinese nationals who have studied or worked overseas in critical high technology areas. When students or entrpreneurs return with skills or knowledge that the central government deems critical they are given free office space in the parks, loans, financial aid, and administrative help in setting up a business designed to bring in foreign investment and technology. Their companies are given tax holidays. Innovative programs such as at Beijing's Zhongguancun High Technology Park and Guangzhou's High Technology Economic and Trade Zone get central government help. These are admirable programs that will develop entrpreneurial skills among well-educated Chinese citizens. However, as students and employees of U.S. companies return home, it is important to know that they are not taking back American economic or military secrets. Good counterintelligence and industrial security programs are very important to U.S. security given this threat.

Mr. Chairman, the enforcement of intellectual property protection laws in China is spotty and inconsistent at best. This is one of the major complaints of American high technology companies about China's compliance with its obligations under the World Trade Agreement. It will certainly be a subject discussed by President Bush and Chinese President Hu Jintao this week. The tendency to steal intellectual property and high technology secrets in China is worsened when ijntellectual property laws are not enforced there. And the problem is further exacerbated when centralized Chinese government programs, such as the "863 Program" I mentioned earlier in my testimony, are specifically designed to acquire foreign high techology with military application. This only creates a climate inside China that rewards stealing secrets.

I believe that U.S. government security, intelligence and law enforcement agencies must focus on the national security. They should be looking for acts of espionage and for violations of the Arms Export Control Act or the Export Administration Act. When it comes to corporate or industrial espionage that is not a matter of national security, I believe that the government owes American companies a good legal infrastructure to protect trademarks, patents and copyrights; a system of education on industrial security; and a strong effort to ensure that China meets its own obligations to create a rule of law that protects the right of ownership and intellectual property. However, I do not believe that American intelligence or security agencies should focus on forms of economic espionage that do not involve national security information. From the standpoint of Congressional action, my view is that the Congress should reconsider the Export Administration Act with a view toward ensuring that its provisions meet the needs of 21st century technology. The 1979 Export Administrtion Act expired in 2001. The Senate passed a new Act in 2001, but no revision passed the House. And the Executive Branch must regularly review the Commodity Control List to ensure that appropriate national security controls on exports do unduly restrict the ability of American industry to compete in the world market. Generally, technologies that are widely available on the world market and

not unique to the United States should not be unduly restricted unless they can be subject to mulitlateral controls.

Finally, we cannot become paranoid and suspect that every traveler, student and businessman from China is a spy or is out to steal technology. Prudent law enforcement programs, counterintelligence programs, security education and industrial securty programs are important means to protect our nation.

Thank you for your invitation to testify today.

Mr. HOSTETTLER. Mr. Anderson.

TESTIMONY OF MAYNARD ANDERSON, PRESIDENT, ARCADIA GROUP WORLDWIDE, INC., AND FORMER DEPUTY UNDER SECRETARY OF DEFENSE FOR SECURITY POLICY

Mr. ANDERSON. Thank you, Mr. Chairman. I too have submitted a statement for the record. With your permission, I will summarize.

Mr. HOSTETTLER. Thank you.

Mr. ANDERSON. Thank you, sir.

We have proved that collectors representing foreign adversaries and friends use espionage, theft and other illegal means to take advantage of the United States and cause unauthorized disclosure of protected information.

We also need to recognize that there are ethical failures of trusted personnel who are prepared to traffic in information and technology because they are greedy or because they are susceptible to foreign pressure, and they are threats as well.

The United States is an open society and a prime target of collectors because it produces more intellectual property than any other nation in the world and does, to some extent, a poor job of protecting it. World changes, producing new alliances and new friendships internationally create more vulnerabilities to our technology. America may have won the Cold War, but we are losing ground economically to those who would pilfer our commercial secrets.

National security and economic strength are indivisible, and the real test in this world of military and economic contests for supremacy may not be who first develops technology but rather who is the first to use it effectively. Technology's application is the key, particularly in an area of dual-use technology.

Integration of the management, protection and use of technology is an objective to ensure that we determine what needs to be controlled, what can be controlled, and employment of the most important control mechanisms. It is imperative that we determine accurately whether any other nation wants our technology and whether any other nation has it already, because we can't afford to spend resources to protect things that don't need protection. We need to balance the protection of real secrets while maintaining the competitive position of American industry in the world market.

It would seem prudent, therefore, to use all current legal remedies available to enforce contracts and personnel actions, to enhance enforcement opportunities against current Government and contractor employees who break trust, to establish new standards and requirements for our foreign visitors, particularly students and researchers, and to ensure, probably most of all, that our citizens know what is expected of them.

The easiest, least-expensive and most effective protection technique is education. All custodians of protected information should be subjected to continuing education concerning threats,

vulnerabilities and protection of information so that they understand the consequences of its unauthorized disclosure, which are obviously jobs, loss of profits and diminished national security.

Everyone should be made aware that national security is every citizen's responsibility.

Thank you, Mr. Chairman.

Mr. HOSTETTLER. Thank you, Mr. Anderson.

[The prepared statement of Mr. Anderson follows:]

PREPARED STATEMENT OF MAYNARD ANDERSON

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.

4.

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.

Mr. HOSTETTLER. Dr. Wulf.

STATEMENT OF DR. WILLIAM A. WULF, PRESIDENT, NATIONAL ACADEMY OF ENGINEERING, THE NATIONAL ACADEMIES

Mr. WULF. Thank you very much, Mr. Chairman, Members of the Committee. I too, like my predecessors here, have a longer statement, which I will submit for the record.

I am pleased to come to the hearing today to remind all the Members of the Committee of the important contributions that foreign-born scientists and engineers have made and continue to make to this country. We are more prosperous and more secure in large part because of them.

Before proceeding, while I don't perhaps have the same credentials in intelligence that my predecessors on the panel have had, I would note that both my wife and I have been advisors to the Department of Defense for decades. We both carry Top Secret SCI clearances and my wife served for 5 years in the Pentagon as the Director of Research and Engineering, where she had responsibility for the oversight of all R&D in the Defense Department.

I am convinced that security, real security, comes from a proper balance of keeping out those that would do us harm and welcoming those that would do us good. Throughout the last century, our greatest successes in creating both wealth and military ascendancy have been due in large part to the fact that we welcomed the best scientists and engineers from all over the world. No other country did that, and nowhere else has the genius for discovery and innovation flourished the way it has here. I am deeply concerned that our policy reactions to 9/11 have tipped the balance in a way that is not in the long-term interest of our Nation's security.

Fifty years ago, our scientific leaders came from Europe. There were the famous names like Einstein, Fermi and Teller, without whom we would not have been the first to have the atomic bomb; von Braun, without whom we would not be ascendant in rockets and space; von Neumann, without whom we would not be world leaders in computing and information technology.

Today, it isn't just Europeans that contribute to our prosperity and security. The names are those like Praveen Chaudhary, now Director of Brookhaven National Laboratory; C.N. Yang, now Nobel Laureate from the Institute for Advanced Study at Princeton; and Elias Zerhouni, who was born in Algeria and is now the Director of the National Institutes of Health.

Between 1980 and 2000, the percentage of Ph.D. students and scientists and engineers employed in the United States, who were born abroad, increased from 24 to 37 percent. The current percentage of Ph.D. physicists is about 35 percent; for engineers, it is over 50 percent. One-fourth of the engineering faculty at U.S. universities were born abroad; between 1990 and 2004, over one-third of the Nobel Prizes awarded to U.S. citizens were to foreign-born scientists. One-third of all U.S. Ph.D.'s in science and engineering are now awarded to foreign-born graduate students.

We have been skimming the best and brightest minds from around the globe and prospering because of it. We need these new Americans even more now as other countries become more technologically capable.

If I have one message to convey to this Committee today, it is that it is a serious mistake to think that all important defense technologies originate in the United States, and hence, the problem is to keep our technology from being stolen by others.

We talk proudly about the MIT "Rad Lab" that developed radar during World War II, but the critical technology came from the United Kingdom. At the end of World War II we were a distant third in the development of jet engines behind both Germany and Russia—the Soviet Union. The World Wide Web was invented in Switzerland, not in the United States. I could go on and on.

Many U.S. corporations are now shifting their development to overseas locations, research and development to overseas locations, not just because foreign labor is cheaper; that is a common and comfortable myth. It is frequently because the quality is better overseas.

Again, real security depends upon a very careful balance, in this case, a balance of openness and secrecy. Walling ourselves off from others, from the otherwise open exchange of basic scientific information, is a recipe for being surprised and disadvantaged.

To be sure, 9/11 and globalization have both changed the balance point. The balance point for the Cold War was a different one than for today. We need to fundamentally rethink our policies. However, in my opinion, several recent policy changes related to visas, to the treatment of international visitors, to this new issue of deemed exports and so on have had a chilling effect.

It has already been mentioned that the applications of international students to attend U.S. colleges and universities has declined. Scientists have chosen to hold conferences in other countries. U.S. businesses have had to shift critical meetings to locations outside our borders. In the meantime, foreign companies, universities and governments are marketing themselves as friendlier places to do business or to get an education. In the race to attract top international talent, we are losing ground.

At the same time, science and technology are growing rapidly in other parts of the world. Over 70 percent of the papers published by the American Physical Society's world leading journal, The Physical Review, come from abroad—70 percent! We do not own all of the science and technology information in the world. It is illustrated by a figure in my written testimony, the number of first degrees in science and engineering awarded per year in Asia is now almost three times greater than in North America.

Permit me to turn to this issue of export controls for a minute. They were instituted in 1949 to keep weapons technology out of the hands of potential adversaries. In 1994, the disclosure of information about a controlled technology to certain foreign nationals even in the United States has been "deemed" to be an export of that technology itself. And recent reports from the inspectors general of the U.S. Department of Commerce and State have suggested that the implementation of the rules governing deemed exports should be tightened.

For example, they have suggested that the exemption for basic research should be altered and possibly eliminated and that the definition of access to controlled technology should be broadened. The university community is rightly concerned that a literal inter-

pretation of the IG's suggestions would essentially preclude foreign graduate students from participating in research and would require an impossibly complex system to enforce.

Given that over 55 percent of the Ph.D. students in engineering in the United States are foreign born, the effect could be catastrophic. Either universities would have to exclude these students, or they would have to stop doing research on potentially defense-related topics, which, of course, includes most of the fastest-moving new technologies. Neither of these alternatives strengthens the United States, they weaken it.

One might ask if these policy changes will improve our security, I would point out that the United States is not the only research-capable country. China and India, for example, have recognized the value of research universities to their economic development and are investing heavily in them. By putting up barriers to the exchange of information about basic research, we wall ourselves off from the results in these countries and slow our own progress. At the same time, the information we are "protecting" is often readily available from other sources.

And finally, in a country with an estimated 10 million illegal aliens, one must wonder whether onerous visa policies or demeaning practices at border crossings will deter the committed trained spy or terrorist from entering the country.

The 2001 Hart-Rudman Commission, which in February of 2001 predicted a catastrophic terrorist attack on the United States, and which then proposed the Department of Homeland Security, said, and I quote, "The inadequacies of our system of research and education pose a greater threat to the United States national security over the next quarter century than any potential conventional war we might imagine." Their essential point is that further damaging our system of research and education, including its relation to foreign-born scholars, is a very dangerous strategy.

The United States still benefits from educating and employing a large fraction of the world's best scientists and engineers. We have great research universities that remain attractive to the world's best and brightest. We are envied for our non-hierarchical tradition that allows young scientists with new ideas to play leading roles in research.

We have progressed because we fostered a tradition of free exchange of ideas and information and embraced a tradition of welcoming talented people from elsewhere in the world. But that advantage is eroding under current and proposed policies.

The international image of the United States was one of a welcoming "land of opportunity." We are in the process, however, of destroying that image, and replacing it with one of a xenophobic, hostile nation. We are in the process of making it more likely that the world's best and brightest will take their talents elsewhere. The policies that superficially appear to make us more secure are, in fact, having precisely the opposite effect.

Protecting Americans from threats must obviously be a high priority. But as I said earlier, real security will be achieved only by a proper balance of excluding those that would do us harm and welcoming those that would do us good by a proper balance of openness and secrecy. With selected, thoughtful changes to U.S.

policies, we can achieve both goals, making our homeland safer and our economy stronger.

I would like to close with another quote from the Hart-Rudman report, "Second only to a weapon of mass destruction detonated in an American city, we can think of nothing more dangerous than a failure to manage properly science, technology and education for the common good over the next quarter century."

Thank you for the opportunity to testify.

Mr. HOSTETTLER. Thank you, Dr. Wulf.

[The prepared statement of Mr. Wulf follows:]

Prepared Statement of William A. Wulf

Good afternoon, Mr. Chairman and members of the Committee. My name is William Wulf and I am on leave from the University of Virginia to serve as President of the National Academy of Engineering (NAE). Founded in 1964, the NAE provides engineering leadership in service to the nation. It operates under the same congressional act of incorporation that established the National Academy of Sciences, signed in 1863 by President Lincoln. Under this charter the NAE is directed "whenever called upon by any department or agency of the government, to investigate, examine, experiment, and report upon any subject of science or art [technology]." I am pleased to come to this hearing today to remind all members of the committee of the important contributions foreign-born scholars, scientists, and engineers have made and continue to make to this country. Foreign-born scientists and engineers have come to the United States, stayed in large numbers, *and we are more prosperous and more secure, in large part, because of them!*

Before proceeding, perhaps I should note that national security is not an unfamiliar subject to me. I have carried a TS/SCI clearance for decades, have been a member of the Air Force Science Advisory Board (AFSAB), and an advisor to DoD on many subjects. When I founded a company in the early 80's, it was based on DoD funded university research, and our principal product was defense-related software. My wife carries more clearances than I, was also an member of the AFSAB, has been a member of the Defense Science Board (DSB) for two decades – except for five years when she served in the Pentagon as the Director of Defense Research and Engineering. I believe it is fair to say that both my wife and I are not only sensitive to national security issues, but for decades have devoted our energies to it. We understand the need to protect certain information, and we value the people who provide us that security and would do nothing that jeopardized them or their mission.

Although I probably don't need to say it to the committee, I want to stress the centrality of our technological prowess to our security. It is said that success has many parents – one example of this

is the many explanations for why we won the cold war. One component of that victory however, was that the Warsaw Pact was never tempted to start a conventional (non nuclear) war even though they had a significant numerical advantage in both troops and armament. The reason was that we offset their numerical advantage with superior technology. Our troops could locate, identify, target and destroy a potential attacker with far greater accuracy, speed, and lethality. MAD (Mutually Assured Destruction) may have prevented a nuclear war, but our "offset strategy" using superior technology was a major component of preventing a conventional one.

It is for this very reason that I am convinced that security – *real* security – comes from a proper balance of keeping out those that would do us harm and welcoming those that will do us good. Throughout the last century, our great successes in creating both wealth and military ascendancy have been due in large part to the fact that we welcomed the best scientists and engineers from all over the world. No other country did that, and nowhere else has the genius for discovery and innovation flourished in the way it has here. I am deeply concerned that our policy reactions to 9/11 have tipped that balance in a way that is not in the long term interests of the nation's security.

Fifty years ago many of our scientific leaders came from Europe. There are the famous names like Einstein, Fermi, and Teller (without whom we might not have been the first to build the atomic bomb), von Braun (without whom we would not be ascendant in rockets and space), and von Neumann (without whom we might not be leaders in computing and information technology). But there are dozens more names, like Bethe and Gödel, that may not be known to the general public, but that formed the backbone of American science and engineering – plus an enormous number of journeymen scientists and engineers whose individual contributions will never be celebrated, but without whom the United States would be neither as prosperous nor as secure as it is.

Today, it isn't just Europeans that contribute to our prosperity and security; the names are like those of Praveen Chaudhary (now director of Brookhaven National Lab), Venkatesh Narayanamurti (dean of the Division of Engineering and Applied Sciences at Harvard), C.N. Yang, (Nobel Laureate physicist, from the Institute for Advanced Study in Princeton), Katepalli Sreenivasan, (recent director of the Institute for Physical Science and Technology at the University of Maryland); and Elias Zerhouni (who was born in Algeria and now is the director of the National Institutes of Health).

Between 1980 and 2000, the percentage of Ph.D. scientists and engineers employed in the United States who were born abroad has increased from 24% to 37%. The current percentage of Ph.D. physicists is about 45%; for engineers, the figure is over 50%. One fourth of the engineering faculty members at U.S. universities were born abroad. Between 1990 and 2004, over one third of Nobel Prizes in the United States were awarded to foreign-born scientists. One third of all U.S. Ph.D.s in science and engineering are now awarded to foreign born graduate students. We have been skimming the best and brightest minds from across the globe, and prospering because of it; we need these new Americans even more now as other countries become more technologically capable.

Top-notch students and teachers from abroad help make U.S. colleges and universities global centers of excellence and diversity. Highly skilled workers and world-class business leaders who come to work with or for U.S.-based companies help keep our economy growing – an amazing fraction of new Silicon Valley start-up companies are headed by individuals born abroad, for example.

It's a mistake to think that all important defense technologies originate in the United States and hence that the problem is simply how to keep our technology from being stolen by others. We talk proudly about the role of MIT's "Rad Lab" in developing radar in WW II – but the crucial technology came from the United Kingdom. At the end of WW II the United States was a distant third in the development of jet engines, behind Germany and the Soviet Union. The World Wide Web was invented at the European

Organization for Nuclear Research (CERN) located in Switzerland -- not in the United States. Again, *real* security depends on a careful balance – in this case a balance of openness and secrecy. Walling ourselves off from the otherwise open international exchange of basic scientific information is a recipe for being surprised and disadvantaged.

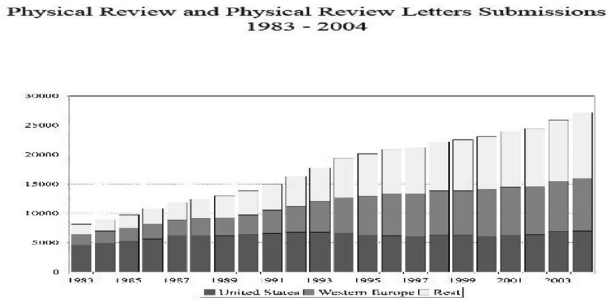
To be sure, 9/11 and globalization have changed the balance point. There is good reason to fundamentally rethink our policies. However, several recent policy changes, related to visas, treatment of international visitors, deemed exports, and so on, have had a chilling effect. Enrollment of international students in U.S. colleges and universities has declined. Scientists have chosen to hold conferences in other countries. U.S. businesses have had to shift critical meetings to locations outside this country. In the meantime, foreign companies, universities and governments are marketing themselves as friendlier places to do business or get an education. In the race to attract top international talent, we are losing ground.

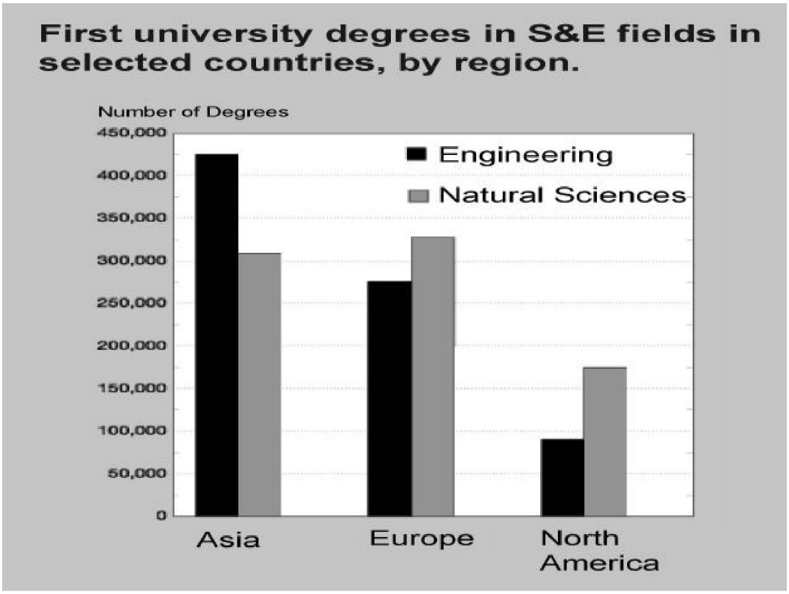
In 1960, none of the present constraints would have had much effect on the flow of outstanding scientists into our country. We were scientifically the most vibrant place in the world, and the best people were willing to make great efforts to come here. That is no longer the case.

After WW II, the U.S. forged a mutually reinforcing triad of complementary R&D strengths in industry, academia and government. However, U.S. industrial laboratories have greatly reduced their support for long-term basic research; and many U.S. corporations are shifting research and development to overseas locations—*not* just because foreign labor is cheaper, as is the common and comfortable myth, but because it is of higher quality! U.S. government laboratories are in various states of disarray, and no longer maintain the stature that they did in 1960's. Government support for the physical sciences and engineering at universities has declined in real terms, and is suffering further under present budget pressures – clearly, a strong research capability is not a current federal priority. Enrollment in the physical sciences and engineering, as a percentage of undergraduates, is among the lowest in the

industrialized world – the U.S. now graduates just 7% of the world's engineers, for example. Given that our 12th graders score among the lowest in the world in science and mathematics, the ranks of U.S. born scientists and engineers are not likely to expand dramatically anytime soon. Our once strong triad of R&D capabilities is crumbling.

At the same time, science and technology are growing rapidly in other parts of the world. Over 70% of the papers published in the American Physical Society's world leading journals, *The Physical Review* and *Physical Review Letters*, now come from abroad. As is illustrated in the second figure below, the number of first degrees in science and engineering awarded per year in Asia (most importantly China) is now almost three times greater than in North America. It is even somewhat larger than in all of Europe. As said earlier, it's a mistake to think that all important defense technologies originate in the United States and hence that the problem is simply how to keep our technology from being stolen by others.





For over 40 years, tens of thousands of individuals at a time have been working in our nation's nuclear weapons program. In that time, no leaks have been publicly proven. The fact that so many people – half of them scientists and engineers, and many of them foreign born – can be trusted with such secrets speaks volumes about the effectiveness of a "culture of openness" in dissuading opportunistic individuals from acting. This culture of openness is characteristic of research laboratories. It means that we talk freely on most things, keeping only very specific controlled information to ourselves. This culture leads to everyone knowing everyone's business, a very effective barrier to unusual or unseemly behavior. This culture is effective in a way that a "culture of secrecy" is not. Most espionage convictions are for individuals working in security agencies, in fact.

Export Controls

Export controls were first instituted in the United States in 1949 to keep weapons technology out of the hands of potential adversaries, but have also been used as an economic tool against our competitors. The export of controlled technology requires an "export license" from either the U.S. Department of Commerce or State. In addition, since 1994 the disclosure of information about a controlled technology to certain foreign nationals (even in the United States) has been "deemed" to be the export of the technology itself. Thus, disclosure also requires an export license.

Reports of the inspectors general (IGs) of the U.S. Departments of Commerce, Defense, and State have suggested that the implementation of the rules governing deemed exports be tightened further. For example, they have suggested that the exemption for basic research be altered, and possibly eliminated, and that the definition of "access" to controlled technology be broadened.

Again, the *real* security of the nation depends upon a proper balance. The university community is rightly concerned that a literal interpretation of the IGs' suggestions would essentially preclude foreign graduate students from participating in research and would require an impossibly complex system to enforce. Further, strict enforcement would undermine the culture that has proven so effective in furthering our security and prosperity. Given that 55 percent of the Ph.D. students in engineering in the United States are foreign born, the effect could be catastrophic. Either universities would have to eliminate these students, most of who historically stayed and contributed to our prosperity and security, or universities would have to stop doing research on potentially defense-related issues – which, of course, includes much of the fastest moving hi-tech technologies. Neither of these alternatives strengthens the United States; both weaken it.

One might ask if these policy changes will improve our security. I would point out that the United States is not the only research-capable country; China and India, for example, have recognized the value of research universities to their economic development and are investing heavily in them. By putting up barriers to the exchange of information about basic research, we wall ourselves off from the results in these countries and slow our own progress. At the same time, the information we are "protecting" is often readily available from other sources. Finally, in a country with an estimated ten million illegal aliens, one must wonder whether onerous visa policies or demeaning practices at boarder crossings will deter the committed, trained spy or terrorist from entering.

We do have important natural advantages.

The 2001 Hart-Rudman Commission, which in February of 2001 predicted a catastrophic terrorist attack on the U.S., and which then proposed the Department of Homeland Security, said:

> "… the inadequacies of our system of research and education pose a greater threat to U.S. national security over the next quarter century than any potential conventional war that we might imagine."

The report was written before 9/11; had it been written afterwards, I am sure "conventional war" at the end of the quote would have been changed to include our struggle against terrorism. The essential point, however, is that further damaging our system of research and education, including its relation to foreign-born scholars, is a very dangerous strategy.

The United States still benefits from educating and employing a large fraction of the world's best scientists and engineers. We have great research universities that remain attractive to the world's best and brightest. We are envied for our non-hierarchical tradition that allows young scientists, with new ideas, to play leading roles in research. We have progressed because we fostered a tradition of free exchange of

ideas and information and embraced a tradition of welcoming talented people from elsewhere in the world. But our advantage is eroding under current and proposed policies.

The international image of the United States has been one of a welcoming "land of opportunity"; we are in the process, however, of destroying that image and replacing it with one of a xenophobic, hostile nation. We are in the process of making it more likely that the world's "best and brightest" will take their talents elsewhere. The policies that superficially appear to make us more secure are, in fact, having precisely the opposite effect.

Protecting Americans from threats must obviously be a high priority. But, as I said earlier, *real* security will be achieved only by a proper balance of excluding those that would harm us and welcoming those that would do us good, by a proper balance of openness and secrecy. With selected, thoughtful changes to U.S. policies, we can achieve *both* goals, making our homeland safer and our economy stronger.

I would like to close with another quote from the Hart-Rudman report:

> "Second only to a weapon of mass destruction detonating in an American city, we can think of nothing more dangerous than a failure to manage properly science, technology, and education for the common good over the next quarter century."

Thank you for the opportunity to testify. I would be pleased to answer any questions the Subcommittee might have.

Mr. HOSTETTLER. At this time we will turn to questions from Members of the Subcommittee.

Ms. Van Cleave, about 30 percent of American university science and engineering faculty are foreign born, according to your testimony, 40 percent of Ph.D.'s in these fields go to foreign students. You also say that foreign intelligence services place senior scientists and exploit academic activities.

Should there be better reporting of what projects these individuals are involved in; and in the case of students, also what subjects they are enrolled in, perhaps through an enhanced SEVIS system.

Ms. VAN CLEAVE. Mr. Chairman, it would be extremely helpful to U.S. counterintelligence to have that kind of increased reporting on these individuals.

Frankly, it is difficult to gainsay the statement that was just made by my fellow panel member here, that what we want to do is exclude those who would cause us harm and welcome those that would do us good. The trick is figuring out which is which.

Mr. HOSTETTLER. It is possible that an individual from a country of concern, if they are applying for a degree in music education, for example, if they start taking nuclear engineering courses as electives, that it would probably be good to know that?

Ms. VAN CLEAVE. It would be helpful to get the kind of reporting of changes in emphasis where students coming for one purpose then are switching their majors or emphasis to areas that might have national security implications.

Mr. HOSTETTLER. But they don't have to be major changes, I mean, if an individual takes, through the course of a 4-year degree, 10 classes in chemical engineering, that doesn't necessarily meet the requirements of a minor in chemical engineering, but it nonetheless will probably be very helpful in their potential work.

Ms. VAN CLEAVE. Yes.

Mr. HOSTETTLER. Thank you.

Your testimony states that Chinese intelligence efforts exploit our open economic system to reduce the U.S. military advantage and undermine our economic competitiveness. It is actually about the only foreign country you have mentioned by name in your testimony. Knowing this, wouldn't you agree that the Visas Mantis clearance needs better vetting by law enforcement agencies, certainly as it relates to a Chinese national coming to the U.S.?

Ms. VAN CLEAVE. Yes, Mr. Chairman. I think that would be very helpful. I appreciate the opportunity that we had in closed session to discuss in more detail some of the reasons why.

Mr. HOSTETTLER. In your testimony, you state that the top 10 collectors probably accounted for 60 percent of foreign collection at defense contractors last year. Could you tell us what countries you are talking about when you talk about the top 10, maybe in the order of their collection?

Ms. VAN CLEAVE. Mr. Chairman, we did have the opportunity to do that in closed session. I am reluctant to do that in open session. However, I am able to tell you some of the reasons why.

A number of the countries that are on so-called "top 10" lists, there is not unanimity across the community about what countries really constitute the top 10. It depends on whether you are looking at incident reports of information that might be amalgamated by

the defense security services, for example, or some of the case loads that the FBI might be reporting; and there is a different way of counting them, and so the top 10 may vary, depending on which source data we are looking at.

But let me give you another reason why I am reluctant to go into certain specifics.

Ms. VAN CLEAVE. Some of the Members some of the member States that are among the top 10 as I believe I mentioned are among some of our close allies, and there are many ways that we deal with these kinds of incidents different from calling them to the carpet in a public forum. There are different kinds of approaches that we might make to allies in trying to forestall this kind of activity. But the Committee can come to its own conclusion and speculation. Those countries that do have particular interests in military build up will themselves be looking for those technologies that can help assist in that military build up, and they will find in the United States a very rich environment in which to acquire those kinds of technologies. It is also the case that there is some measure of economic competition that drives technology acquisition where there is commercial advantage to be gained and a lot of money to be made that is yet another incentive, and so we see a great deal of activity to include many countries beyond just the top 10, but indeed at least a hundred nations. Nationals from a hundred different nations were recorded just last year in targeting U.S. technologies.

Mr. HOSTETTLER. Ms. Van Cleave, I appreciate the point that you made with regard to our friends. Actually, in your oral testimony you did mention two of those nations, China and Russia. Our largest—well, I should say one of our largest trading partners—we have ongoing evolving relations with Russia. The reason why I asked the question is the exact reason you gave why you say you are reluctant to give us that, and that is, there is an assumption among many of our constituents, many of our citizens of the United States that our friends don't spy against us. But as you mentioned, in general, that is a very erroneous assumption to be made. And the reason why I asked you that question is to put on the record very specifically who those people are because, once again, it's important for us to know that, for example, through the Visa Waiver Program, and through other programs that don't take advantage of the Visa Mantis system, that there may be requirements for us to change the law with regard to our friends. And I mean, I don't mean that with quotation marks. I mean friends but that have reasons that may be confusing to a lot of us and would be very confusing to a lot of my constituents as to why they aggressively commit espionage against the United States. And so I will not press you on the issue, but I will simply, once again, reiterate that it's important for us to, in open session, if it is not classified, to divulge this information really for the benefit of this Committee and the benefit of our constituents.

Dr. Wortzel, your testimony states that tens of thousands of student visas were given to Chinese nationals last year; in fact, one of the highest. Do you believe we're giving preference to China in these student visa numbers over our allies, over some of our allies?

Mr. WORTZEL. I don't think it's a definite preference toward China. I think what you're seeing, first of all, 1.3 billion people there, there's going to be more students trying to get out. We're obviously a very attractive place to get an education, whether it's a high technology education or an education out in the social sciences. I think our programs are actually pretty restrictive. It's difficult to go into an American Embassy and get into the United States if you're in China. So I think we have to deal with the fact that there are just huge numbers of people there. India, only second to that, and that probably accounts for the numbers.

Mr. HOSTETTLER. Do you believe an enhanced SEVIS system would allow us to gain better information to provide our intelligence community the information they need to——

Mr. WORTZEL. I do. I'm a great advocate of data mining. I think that the ability to electronically sort through what is open-source data, who's here, what are they doing, whether that's by someone in immigration—they've got a right to know what somebody's doing at a university. Now, one can argue that a U.S. intelligence service getting that information might be objectionable to a university president. But if the immigration service gave somebody a visa, I think it'd be great to allow them, allow Customs to get in, or Immigration, I'm sorry, to get in and say, okay, we gave Joe Doe a visa, and he said he was coming here to study this. Let me see what he's studying. And those are things that can be done quickly, electronically, and things can be sorted out. I do think we should be approaching it that way, and I think that we have appropriate agencies in the Government that could look at that, and then if there's a reason to raise concerns about what's going on, they turn it over to another agency or counter-intelligence agency.

Mr. HOSTETTLER. Very good. Without objection, I will grant the Chair an additional minute to ask one additional question of Dr. Wulf, maybe a couple of questions actually. Very short answers. You might not have the information. Dr. Wulf, could you tell me, given the fact that Master's and Ph.D. slots for engineering are limited in the United States, would you have statistics that tell us the number of American citizens who are denied Master's applications, who have Master's applications denied, as well as Ph.D. applications denied in the United States? Would you happen to have those?

Mr. WULF. Approximately zero.

Mr. HOSTETTLER. So it's really unlimited—the number of Master's and Ph.D. slots?

Mr. WULF. I didn't quite say that. But the number of Americans who do not enter graduate programs because there's no space is essentially zero.

Mr. HOSTETTLER. Okay.

Mr. WULF. The trouble is they're not applying.

Mr. HOSTETTLER. So there are zero denied.

Mr. WULF. Yeah. Approximately zero. I mean, there may be some oddball cases I don't know about.

Mr. HOSTETTLER. Thank you very much.

The Chair recognizes the gentlewoman from Texas, Ms. Jackson Lee.

Ms. JACKSON LEE. Thank you very much, Mr. Chairman. Your initial round of questioning certainly points to a dilemma which we face. I'd like to take some remarks that were made generally speaking through the testimony presented in the open session to indicate my agreement. Let me first of all thank Congresswoman Lofgren for recognizing Dr. Wulf and the astuteness in which she recognized you in as much as you are representing or certainly associated with the University of Virginia, and I couldn't think of a better school. I happen to be an alumnus. So I thank the Congresswoman very much for her astuteness, Dr. Wulf, and I thank you for your service, as well as I do the other panel members.

But you did highlight for us the fact that we do prosper because we skim the best scientists from around the world. At the same time, I think interwoven into your remarks is the idea that we suffer as well from enticing students and graduate students into the sciences and other high technologies that are necessary. So I'm going to come to you and pose that question. But I do want to go to Ms. Van Cleave to ask, what is the extent that she feels that we are now able, the United States, your industry—your, in terms of counter intelligence—able to identify, right now, foreign nationals who are coming into the United States to engage in espionage? Do we have that capacity?

Ms. VAN CLEAVE. We have limited insight into the foreign intelligence operations into the United States, which is to say, to the extent that we understand the character, make-up and operations of foreign intelligence services of concern, we can identify individuals that might be sent here for those particular purposes. However, much of the intelligence collection against the U.S. technology base is carried out not by known intelligence officers but rather by those who are employing nontraditional collection means against us. And that is a much much more difficult problem.

There I would have to say that we have precious little understanding or way of knowing when individuals who ostensibly are coming here for legitimate business purposes might, in fact, have more troubling objectives in mind.

Ms. JACKSON LEE. So, in essence, part of the road map that you're providing for us today is the heaping up, if you will, of resources to look at that component that would be nontraditional in the way that they would seek to secure information. That seems to be where we need some emphasis.

Ms. VAN CLEAVE. Yes. We're very much in need of tools that would enable us to be able to characterize who those people are and why they are here, that small slice that is here for illegitimate purposes.

Ms. JACKSON LEE. I thank you.

Dr. Wortzel, I likewise had some agreement with some of the remarks that you have made. But let me just say, and I believe that we will wind up on the same page. We know that, as I started out by saying, the importance of the intellectual exchange and the benefits that the United States has gained by a vast number of individuals. And we also know, without any naming or, if you will, illuminating any closed sessions, we know that even our allies have been found to be engaged in some activities that we would not support. So I don't want this to be a hearing that stigmatizes the en-

tire student body from China. They our allies and friends. We have engaged in some very positive exchange opportunities, both in terms of our student exchange but also our trade exchange. And frankly, we are working toward a diplomatic relationship in terms of their continuing improvement. And I might add, we certainly want to ensure that our military operations are more in sync than in conflict. But you did mention, and I was trying to find your quote, but let me just say this: I look at it that the overall war on terrorism has taken us away from—and don't want to suggest that we should diminish that effort, but we need to increase, if you will, the resources for the rest of the intelligence community. Why don't you comment on where we need to, if you will, lift that issue up? And in the meantime, I'll be finding one of the quotes that I agree with you on. And I guess it is the point that you made about our work should be—that ties into my question—national security, versus the question that many Members—rightly so, because their constituents are impacted by this whole economic issue. If you go to China, you're inevitably talking about CDs and country western music and other music that they have obviously utilized. But that's economic. And I think you said something about, we should be focusing on national security. Can you share that with me?

Mr. WORTZEL. Well, I think we should—thank you, Congresswoman. We should focus on national security. We need to provide, as I said in the testimony, the legal structure here in the United States, and we need to foster a legal structure in China that will provide for property rights and intellectual property rights. But we need to worry about national security here. And I think that's the critical task. Refining the lists of controlled commodities, dual-use items, to ensure that we protect what is really unique to the United States. I mean, there are some things we're just way ahead on that nobody else is doing, composites that make stealth technologies, turbine and in jet engine technology. Nobody else does this. We need to think about that. I would argue generally that basic research in universities has got to be open, wide open, but that when the Department of Defense or the Department of Energy goes to a specific university and funds a program that moves into applied research, then we should be able to know who's working on it and what they're working on and why they're there. So I wouldn't worry, Mr. Chairman, about somebody taking 10 courses in chemistry, advanced chemistry. But if he or she is working to do research on an applied technology with military application or with application for weapons, I'd get really nervous about it. And I would want to be able to know that.

Ms. JACKSON LEE. Mr. Chairman, Dr. Wulf, if he might respond to the question I raised. Dr. Wulf, that was the question dealing with—I started out the whole question dealing with the importance of the talent that comes here to the United States and the lack of U.S. Citizens engaged in the sciences.

Mr. HOSTETTLER. No objection. The gentleman will be allowed to respond.

Ms. JACKSON LEE. I thank the Chairman, and I'll conclude with that.

Mr. WULF. As I said in my oral testimony, and it appears again in my written testimony, foreign-born nationals represent an enor-

mous fraction of the science and engineering talent in this country. I tried to give some examples. The fact that somewhere between 25 and 30 percent of the faculty in engineering schools are foreign-born, the fact that overall, something like 37 percent of all of the engineers and scientists in the United States are foreign-born, the fact that a third of the Nobel Prizes awarded in the last 10 or 15 years to U.S. Citizens were to foreign-born. It's just really hard to overstate the benefits that we have reaped by skimming off the best and brightest minds from around the world. And we are, in my opinion, in serious danger of creating an atmosphere that those people will not want to put up with.

Ms. Van Cleave made reference to the fact that, in the fifties, a number of Chinese returned to mainland China and set up their missile program. I would recommend to any Member of the Committee that feels like exploring that, that they take a look at a book called, The Thread of the Silk Worm, about the man who headed the Chinese missile program, named Tsien Hsue-shen. He was a professor at Cal Tech, got his Ph.D. at MIT, was one of the leading rocket scientists, literally, in the United States, and quite improperly and erroneously, got caught up in the McCarthy hearings, was held in house arrest for, if I remember correctly, 2 years and, finally, in disgust returned to China and created the Chinese missile program. Yes, it was a returned Chinese. But we drove him there.

Mr. HOSTETTLER. Will the gentleman concede the fact that it was the Communist Chinese missile program?

Mr. WULF. Oh, yes. Absolutely.

Mr. HOSTETTLER. The Chair now recognizes, without objection, the gentleman from Texas for questions, 5 minutes.

Mr. GOHMERT. Thank you. Appreciate my colleague allowing me to proceed.

I'm going to ask each of you to name the top two immigration practices or omissions that you believe are the biggest threat to our national security. But while you're thinking about that, I want to ask Ms. Van Cleave, are you familiar with the diversity visa program where we provide 50,000 visas a year on the basis of a lottery? Are you familiar with that program?

Ms. VAN CLEAVE. Congressman, I have to say, no, I'm not.

Mr. GOHMERT. Okay. Well, then I don't guess you can tell me how many terrorists may have utilized that program. But anyway, I would suggest that you take a look at it. Some of us, we voted that out of this Subcommittee, a repeal of that, because it seemed ludicrous to some of us that we be awarding visas on the basis of a lottery, allowing immigration to abdicate their responsibilities. That's a concern of some of ours. But let me start with Dr. Wulf and work our way down to my left. Doctor, what do you see as the two biggest, two immigration practices or omissions that are the biggest threat to our national security?

Mr. WULF. Two? That's not easy. But the first one I would name is the fact that immigration visas are not awarded particularly on the basis of the contribution which the individual will make to the country. They are more typically family based or that sort of thing. I think we ought to give special consideration to those people who can really contribute to the country. And I have to say, the second

one is overreaction. I really am concerned that we're in the process of making things worse rather than better by overreacting.

Mr. GOHMERT. Thank you.

Mr. Anderson.

Mr. ANDERSON. Yes, sir. I think perhaps the most important one to me is that we don't know who is arriving here. We do a lot of sort of superficial work, but we're rather poor in determining just exactly who's coming. And I don't mean to—I don't mean for that to sound discriminatory. But we don't ask those folks, for example, students and researchers coming in, we don't ask those folks to provide us with a great deal of information about who they really are. We ask it of our own students. We ask it of our own military personnel. We ask it of all kinds of people in the United States, but immigrants really are not subjected to very strenuous questions on who they are really. And I think that may be, to my mind, the greatest one. I'm not sure that—I'm not sure that I could name a second one. I don't like quotas. I don't think quotas are good. I don't know that that's a—I don't know that that's a threat to us. But I think a failure to really identify our immigrants is a major issue.

Mr. GOHMERT. Okay. Thank you.

Ms. Van Cleave.

Ms. VAN CLEAVE. From the perspective of counter intelligence, immigration laws are very clear: where we have an individual who may be known or expected to engage in intelligence activities and activities inconsistent with U.S. laws, visas are denied. But my real concern about immigration laws is that, from a CI perspective, they really can't do a great deal for us beyond that. I mean, there isn't a panacea that enables or immigration laws to protect us against all of the things that this hearing has now convened to discuss. I would have to say that getting at the real question of who these people are who are coming into the United States, immigration laws can do, can provide some of that information to us. But that really is the point where I think that we need to have a layered approach of which immigration controls are only one part. The matter that was mentioned a little earlier by the Chairman——

Mr. GOHMERT. Can you help me? Maybe my mind's eye is too simplistic. I'm just asking you, what do you see as the biggest threat to national security? And from a counter intelligence—you're saying we need a layered approach.

Ms. VAN CLEAVE. Because, sir, I know——

Mr. GOHMERT. So the biggest threat in your mind is that we don't have a layered approach?

Ms. VAN CLEAVE. I know that foreign intelligence services and foreign governments will exploit such loopholes as they can find to send personnel here to achieve certain ends.

Mr. GOHMERT. Bingo. That's what I'm looking for. What loopholes do you know of that we can fix? Number one problem. Number two problem.

Ms. VAN CLEAVE. And I believe in closed session I was asked to take, for the record, that particular question and to provide a detailed answer back to the Members of the Committee. But in open session, let me say that I am concerned that, where there is an opportunity that immigration laws present for foreign nationals to

enter here because they present themselves as residents of another country, and we really don't get true disclosure on who they are and where they really come from, then that is one particular type of a loophole that I think that this Committee may want to consider closing as it is reviewing our immigration laws.

Mr. GOHMERT. So we don't get sufficient information on where this individual is actually coming from. Is that correct?

Ms. VAN CLEAVE. In certain instances, that is correct.

Mr. GOHMERT. Number one. I wasn't asking anything classified. Just a succinct, what do you say, number one problem, number two problem, and then we can go to work from there. We can get classified information. We can go beyond. But okay, so that's the number one problem. Sufficient information on where they're from. What else?

Ms. VAN CLEAVE. With respect to other aspects of our immigration laws, I have to tell you, if it isn't obvious already, that I am not an expert in U.S. immigration laws.

Mr. GOHMERT. You're hopefully an expert on counter terrorism or counter intelligence.

Ms. VAN CLEAVE. Yes, sir. That's correct. That is correct. And being able to avail ourselves of different kinds of databases and information insights on persons who are coming into the United States in various categories of immigration visas is very valuable to U.S. intelligence. And to the extent that we can have more robust databases on persons who are coming here and what they do while they are here, it is of help to us very much.

Mr. GOHMERT. And I apologize to you if you felt like I was trying to make you into an expert on immigration. And I apologize if I presumed too much in thinking that someone in counter intelligence might overlap or bump into areas of immigration policy where a light would go off and you say, oh, that's bad for our country that we have this policy. It bumps up against everything we know to be true and good as counter intelligence. Some of us may individually be counter intelligent. But anyway, Dr. Wortzel, if you would, very quickly. My time is up.

Mr. WORTZEL. I think that the Technology Alert List and the Visa Mantis program as a process is a good idea. I think it can be improved by education for the officers that actually stand the visa line. And my own experience in embassies is that, when you have an ambassador that insists on interdepartmental cooperation and screening of visa applications, you end up with better educated selections of who's getting a visa and who's getting denied. So I would improve that. It's something I think we're doing well. I think one of the greatest threats is that when we make it too difficult for an American company to bring in an intra-company transfer, either to do work in the United States, or for a corporate education program, we force that company to export its entire R&D effort to a third country or to China, a place like China. So I think we have to be very careful about this balance of what I just advocated in Visa Mantis and Technology Alert Lists and ensuring that when a company has a legitimate need for some foreign expert to come in here and get educated or do research and go home and manage or to work here, we don't force that company to export our R&D capability outside of United States.

Now, Mr. Chairman, I failed to respond to one part of Ms. Jackson Lee's question. And if you would indulge me, I could do that in a minute.

Mr. HOSTETTLER. Without objection.

Mr. WORTZEL. Certainly. She asked about the balance between counter intelligence responsibilities and antiterrorism investigative responsibilities for the FBI. And let me say that my experience before and after September 11, 2001, in having to deal with FBI agents here in this country that you know I may have spoken to or may come to interview me is they're doing a pretty good job. I mean, these—they are able, despite the fact that they're out hunting terrorists and hunting people that are perhaps dealing in weapons of mass destruction, they're still able to focus on the big ball park issues that deal with what may be Chinese espionage, so that their people can use more reinforcement. I think they need more counter intelligence agents in the field. They can use more education. I find myself talking to FBI counter intelligence agents that don't know the history of espionage with China, and you know I'm going back over the fact that I'm a little older, and I've been part of it. But basically, I'm pretty happy with what they're doing as an agency, and I support the changes in the creation of a new division.

Mr. HOSTETTLER. Thank you.

The Chair recognizes the gentlewoman from California for 5 minutes, Ms. Lofgren.

Ms. LOFGREN. Thank you, Mr. Chairman.

I want to focus a little bit on the Visa Mantis process because it is bulky and it is slow and it's causing us problems. And I'd ask unanimous consent to enter into the record an article from the New York Times this August that talks about a Ms. Wang, who is a cryptographer, mathematician actually, who was one of nine invitees to a conference on cryptography that was going to help the United States because they found a flaw, and they were going to help us. And they were not able actually to get in to provide that help.

Mr. HOSTETTLER. No objection.

Ms. LOFGREN. I'll just note also, last spring, I met with, I won't mention his name but a Nobel Prize winner in California, who told me that he will no longer organize scientific conferences in the United States because you can't get the scientists in. And so I've actually, since he said that I've been looking at all the high energy physics, it's all, it's in Toronto, it's in Europe. They're not here anymore. And so we're going to pay a price for that. The Visa Mantis, stepping back, I think someone said we need to take a look at our export control system. And I do—we've tried to do that. We lost a vote on the floor here. Secretary of State Rice suggests we ditch the MTOP standard—it doesn't work—and to go with a standard of what's readily available, which makes a lot of sense to many of us. If we were to do that, here's the question: Wouldn't that help on the Visa Mantis project? Because then you would have a much limited set of technologies, and you would be protecting it against the things you really needed to protect, instead of this broad area of when you go to Fry's Electronics and buy it, and if you can buy it at Fry's, it's too late. And then, wouldn't that also help on the deemed export problem? Because right now, we are controlling on

things that—I mean these students are just going to go and get the same thing at Oxford, or you know, it's not as if we're the only people that are studying this. What is your reaction on that approach as part of the way to fix the Visa Mantis problem?

Mr. WORTZEL. First of all, on MTOPS, I would drop that, too. I think it's kind of silly to begin control and speed—I think you have to begin to figure out if there are certain software applications that have great military or cryptographic application that you control. And I think it's getting silly to control MTOPS, and I think it's getting silly to control chip fencing, whether it's five or 13 microns or whatever. Now, all these questions that you're asking really also come down to questions on deemed exports. And well, let me give you an example. You can study this stuff. I'm a political scientist. I'm a military officer. You know, I have done a little bit of intelligence work here and there. I'm not an engineer, and I never worked in production. And frankly, most consular officers on a visa line have not either.

Ms. LOFGREN. They don't know.

Mr. WORTZEL. They don't know. So their education is a very important part of it. And here, if you're working in an embassy, if you have got a good ambassador or consul general he's putting those people in touch with the industry people.

Ms. LOFGREN. Let me just—I know I'm going to run out of time. I don't want to be rude. But right now, we have the responsibility; the State Department with Commerce does this whole list. Just simply by shrinking the list we would help the situation to target, it seems. Would you agree Dr. Wulf?

Mr. WULF. As long as you shrink it by making it more specific. Part of the real problem is here it's a long list or its two long lists, and each item on the list is quite generic. So you hand this to some poor consular official who doesn't have a technical background, and they——

Ms. LOFGREN. Yes it is always easier to say no. You don't get called to account for saying no. Only for saying yes.

Mr. WULF. Right.

Ms. LOFGREN. The other thing I had, looking at it, the slowest part of the whole Visa Mantis program is the FBI. They don't have a deadline. And I've often wondered, how much do they really have to do? I mean, these are foreign nationals. They haven't in most cases been to the U.S.; they're not permanent residents. They don't live here. You know, maybe the CIA might have something on them, in which case we should get that information. But they're not going to be on a rap sheet in the FBI's computer. I mean, it just seems to me that if you're paying a price by having the top scientists go to other countries, having your scientific conferences be shoved abroad, or I'll tell you, as I was driving to the airport in California, I heard an interview of one of my constituents who had a huge telephone network system that he had sold to a company abroad. He couldn't get his customer in to teach them how to use the system, so he relocated his company to Vancouver and left California. So there's a price to be paid on all of this. What are we getting for it in terms of security?

Mr. WORTZEL. Well, first of all, I don't think it's wrong to ask universities and companies to plan ahead and figure out who

they're going to invite. So a few months advance notice, you know, if you decide tomorrow morning you're going to run a conference and you want somebody——

Ms. LOFGREN. Right. No. I don't disagree with that.

Mr. WORTZEL. With respect to—I wouldn't eliminate any part of our intelligence or law enforcement community. But I do think that of all the agencies, from what I have seen and read and experienced, that's the one that can profit the most by a systematic automation of the records.

Ms. LOFGREN. Well, it's paper records, and that's why it takes so long. I mean, it's pretty shocking that they've still got paper.

Mr. WORTZEL. So I wouldn't eliminate it. Instead, I mean, you have oversight. That's where I would push for.

Ms. LOFGREN. We've yet to have a hearing on oversight of the FBI in the Full Committee in the 10 years I've been on the Judiciary Committee. I would just close. I know my time is up. We talked about our competitiveness. But if 2 percent of the population of China is really, really smart, that's more than the entire population of the United States. So that's what we're competing against, and we'd better make sure that we've got new Americans to do that. And I yield back.

Mr. HOSTETTLER. I thank the gentlewoman. The Chair recognize the gentleman from Iowa, Mr. King, for 5 minutes.

Mr. KING. Thank you, Mr. Chairman.

I regret that I had to step out of this hearing for a period of time, and I missed some of the core of the testimony of the witnesses. I thank you all for your testimony and your written testimony. I have absorbed some of this testimony when the doors were closed and some of it when it's open. And I look back at the United States of America in 1959, and I remember sitting in the sixth grade when Sputnik went up into space. I didn't know at that day, but I found out over the years that I had been assigned to, and millions of American students had been assigned to, go down the path of science and technology and engineering and math and chemistry. And it was, we did an all out full court press. We mobilized America to educate our young people so that we could prevail in the race to space, and in the process of doing so, we also, I believe, laid the groundwork to prevail in the Cold War by succeeding economically where the Soviet Union was bankrupted and before they checkmated us militarily, by the way. And that backdrop of the history of what we did in this country to mobilize a nation of essentially U.S. citizen students that went into the science and technology was the pattern that we had in the past. And I would ask, to what level we have a truly, an intellectual exchange when we have, I think, far more students here in the United States studying science and technology than are studying in foreign countries? Is it an exchange, or is it just a transfer of our science and technology to foreign countries? And then, so then I began to think in terms of what's ahead of the next generation of America if we're watching these numbers grow. And as Dr. Wulf has testified, 25 to 30 percent of the engineering faculty is foreign-born; 37 percent of the engineering degrees are foreign-born; one third of the Nobel prizes are foreign-born. If that number is growing, and I suspect it may be, because more than 50 percent of the engineering doctorates are

foreign-born. So are we, do we have an intellectual transfer here, or are we just slowly transferring our intellectual property and our human property to foreign countries? A generation from now, are they going to need our universities to teach this, or are they going to have then established in place an ability to teach that engineering? Are we going to send our students there at some point? At what point do we reach that critical mass, that tipping point where they're not coming to the United States, not because we haven't set a climate that says, please come here and learn, but because they have now absorbed the science and technology necessary for them to be the world leaders? And if we're looking at a nation like China, for example, that has 1.3 billion people and the ability to mobilize all of them if they choose or skim the cream off of the crop, get that education, bring them back home again, have we already marketed some of America's future? And what if—and so within the context of that, that generational, what happens in 25 years or 30 or 50 years? I inject another question. And that is, are the Israelis educating Palestinians or Arabs in military or nuclear technology or missile technology? Do they have an exchange program going on with their neighbors, their people that are sworn to kill them and drive them into the sea? I mean, that's a little microcosm possibly of this, I'll say, the risk of an impending crisis with China and a generation from now. So if the Israelis see the wisdom in not doing that with their neighbors sworn to their annihilation—and I remember the Chinese general that threatened to nuke Los Angeles. And I wish Mr. Gohmert were here, because he had a conversation with their leadership over there last month to point that out. I pose then my question to Mr. Wortzel. Are we thinking generationally in this? And what would happen to the future of this country if we decided that we didn't want to take a security risk or intellectual property risk and wanted to mobilize the young people in this country like we did after Sputnik?

Mr. WORTZEL. Well, I would like very much to see scholarships targeted toward American students rather than bringing foreign students into American universities. Particularly when you're dealing with a country that has 790 something—or $43 billion in foreign reserves. They can afford to send their own students to American universities. But frankly, I would not keep them out. We do not know the ultimate result of our engagement policy with the People's Republic of China. It is a latent security threat, and it is certainly a real threat in the sense of its strategic nuclear forces programs not so much in its conventional forces. But I will tell you that there's great change there. The economic freedom is opening up. It hasn't resulted in a change in political freedom. You find the average, the average Chinese citizen in most urban areas, and now that's the majority of them, owns an apartment. They have a mortgage. You know, I mean, it's changing. So we don't know what the outcome will be. I think what we need to do, again, is to identify the most critical technologies and military systems—well, not military systems—but military, dual-use technologies where the United States is so clearly ahead and ensure we protect them. But we should not be protectionist about keeping Chinese citizens out of this country or out of our universities.

Mr. KING. Thank you.

Dr. Wulf.

Mr. WULF. I think we all should put emphasis on how we get more U.S. students to study math and science. Just as you pointed out, post-Sputnik, it became a national priority, and by George, a whole bunch of people from my generation took math and science, became engineers and scientists. And we're living off of them now. The trouble seems to me, is that science and technology is not particularly a priority in this country right now. I just got a letter to make a nomination for the Millennium Prize. This is a million euro prize that's put up by the Finns. Now if I remember correctly, there are 4 million Finns. So it's kind of a third of New York City. And they put up a yearly million euro prize. We haven't awarded the National Medals in Science and Technology for the last 3 years. We've named them, but they haven't been awarded. It's not been enough of a priority for the President to do that. We have our funding for physical science and mathematics, engineering research has been flat or declining for 2 decades. Total research budget is going up, but it's all going into the life sciences—I just read this—as our society as a whole doesn't believe that is a priority. And boy that's communicated to the young kids, and they don't see that they should be doing all that hard work when there's no reward for it.

Mr. KING. Thank you.

Thank you, Mr. Chairman. I yield back.

Mr. HOSTETTLER. I thank the Chairman.

Ms. JACKSON LEE. Mr. Chairman, would you yield for just a moment?

Mr. HOSTETTLER. Yes, I yield to the gentlelady.

Ms. JACKSON LEE. Dr. Wulf posed this question before, and I won't ask you to repeat it. I'll just make this statement because I heard your answer to Congressman King's comments. This is not the Science Committee. Both Congresswoman Lofgren and myself are Members of the Science Committee. And I would simply say that the dearth and the problem is even wider than you might have expressed here. There has to be a parallel effort in order to surpass or to overcome the dilemma that we're in. National security, more resources in intelligence, but over here, a ramping up of the training of Americans in the sciences and the mathematics and the encouragement of grad students and professors and researchers and more dollars in basic research. Thank you.

Mr. HOSTETTLER. The Chair feels compelled to make an addition to the record given my background. Being an engineering student in the late seventies and early eighties, I can't remember a single Federal Government program that encouraged me to become an engineer. I do remember the influence of family and community and of the economy and the fact that I was encouraged to follow my desire to study that which I enjoy which is math and physical sciences. It just so happened that my graduation also coincided with one of the largest build-ups of the United States military where there was a huge demand for the applied sciences. And the fact that I also graduated at a time when the nuclear industry was, had gained ground. But as a result of a very limited number of unfortunate incidents in that industry, caused that industry to almost evaporate from future growth. Virtually all of my encouragement came not from the Federal Government, but came from a robust

economy and a strong understanding of the strong national defense, which all of those needed engineers, and there was a tremendous demand for that. I think if we see a, I think we can—it's inversely proportional to the level of attendance that's been taken on by the Federal Government. Since I have been in Congress, as an engineer, I've heard continually about this, about the fact that we're spending more in the Federal Government on attention to science and engineering and that we are getting fewer American scientists and engineers. It made, once again—this is not, to reiterate, this is not the Science Committee. But this is a Committee that is going to look into in the coming months the issue, one of the issues that was touched on briefly here, and that is how we—what is the relationship between foreign-born, foreign nationals and our institutes of higher learning with regard to engineering and science and why people aren't doing what they did in the late 1970's, and that is going into engineering in fairly large numbers. If I remember, the fact that there were a few people that were kept out of the programs because of restrictions on attendance at that time. So I just make that addition simply out of experience.

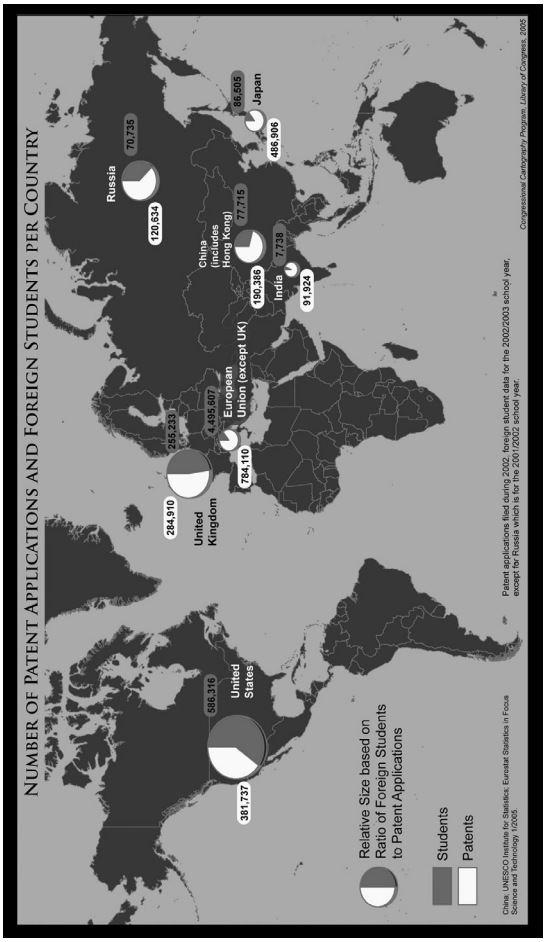
And I appreciate the input of all the members of the panel. Your testimony has been highly effective and highly beneficial to this discussion. All Members will be allowed 2 days to make additions to the record. The business before the Subcommittee being complete, we are adjourned.

[Whereupon, at 4:11 p.m., the Subcommittee was adjourned.]

APPENDIX

Material Submitted for the Hearing Record

Map on the "Number of Patent Applications and Foreign Students Per County," submitted by the Honorable John Hostettler, a Representative in Congress from the State of Indiana, and Chairman, Subcommittee on Immigration, Border Security, and Claims



PREPARED STATEMENT OF THE HONORABLE SHEILA JACKSON LEE, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF TEXAS, AND RANKING MEMBER, SUBCOMMITTEE ON IMMIGRATION, BORDER SECURITY, AND CLAIMS

The subject of this hearing is, "Foreign Nationals Engaged in Economic and Military Espionage." According to the National Counterintelligence Executive Office's report to Congress this year, individuals from almost 100 countries attempted to acquire sensitive United States technologies in FY2004. The report concludes that foreign access to sensitive information with both military and commercial applications has eroded the United States military advantage, degraded the U.S. Intelligence Community's ability to provide information to policymakers, and undercut U.S. industry.

The report states that we are vulnerable to such espionage because the openness of the United States has provided foreign entities with easy access to sophisticated American technologies. New electronic devices have vastly simplified the illegal retrieval, storage, and transportation of massive amounts of information, including trade secrets and proprietary data. Globalization has mixed foreign and American companies in ways that have made it difficult to protect the technologies these firms develop or acquire, particularly when that technology is required for overseas operations. Lastly, sophisticated information systems that create, store, and transmit sensitive information have become increasingly vulnerable to cyber attacks.

Apparently, the Counterintelligence (CI) Community is uncertain about exactly how much of the intelligence collection effort is directed by foreign governments and how much is carried out by private businessmen, academics, or scientists for purely commercial or scientific purposes. It is clear, however, that some foreign governments do employ state actors. This includes their intelligence services as well as commercial enterprises. Most of the foreign governments that are attempting to acquire American technology employ tools and techniques which are easy to use, inexpensive, low risk, and sometimes legal. In most cases, foreign collectors simply ask for the information via e-mail, a phone call, a FAX, a letter, or in person.

The report asserts further that increased demand for foreign labor in United States high-tech industries and the sharp rise in foreign investment in the United States over the past decade have given foreign governments increased access to American businesses and, consequently, to U.S. trade secrets. In addition, recognizing the mutual benefits of an unhindered exchange of information, the United States opens its military bases, national laboratories, and private defense suppliers to foreign visitors. There were more than 14,000 requested visits to official U.S. facilities in FY2004. Although facilities hosting foreign visitors generally employ security measures to minimize the loss of trade secrets and sensitive technologies during these visits, the CI Community continues to see reports of losses.

These are real concerns. Nevertheless, the visits from foreign nationals are valuable to American companies and the United States government. Also, many American industries need highly educated professionals from other countries. The employment of such foreign professionals has increased American productivity and resulted in more jobs for American workers. In the science-oriented sectors, for instance, employers often need a professional with cutting edge skills and unique expertise and find that qualified American workers are not always available to fill these positions. In other fields, such as education, shortages exist in specific areas of the country and positions continue to go unfilled.

Foreign students represent half of all United States graduate enrollments in engineering, mathematics, and computer science. We do not have enough United States students graduating with advanced degrees to fill the highly specialized positions and, according to the Bureau of Labor Statistics, the demand for these graduates will increase.

Foreign countries, such as Germany, have updated their immigration laws to attract highly educated talent. If our immigration laws do not allow these professionals with cutting edge knowledge to remain in the United States, they will go to work for our competitors and additional jobs that could have remained in the U.S. will follow them abroad. The result will be American jobs lost and American projects losing out to foreign competition.

Thank you.

NEW YORK TIMES ARTICLE SUBMITTED BY THE HONORABLE ZOE LOFGREN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF CALIFORNIA

Copyright 2005 The New York Times Company
The New York Times

August 17, 2005 Wednesday
Late Edition - Final

SECTION: Section C; Column 1; Business/Financial Desk; Pg. 4

LENGTH: 852 words

HEADLINE: Chinese Cryptologists Get Invitations to a U.S. Conference, but No Visas

BYLINE: By JOHN MARKOFF; Chris Buckley contributed reporting from Beijing for this article.

DATELINE: SAN FRANCISCO, Aug. 16

BODY:

Last year a Chinese mathematician, Xiaoyun Wang, shook up the insular world of code breakers by exposing a new vulnerability in a crucial American standard for data encryption. On Monday, she was scheduled to explain her discovery in a keynote address to an international group of researchers meeting in California.

But a stand-in had to take her place, because she was not able to enter the country. Indeed, only one of nine Chinese researchers who sought to enter the country for the conference received a visa in time to attend.

Although none of the scientists were officially denied visas by the United States Consulate, officials at the State Department and National Academy of Sciences said this week that the situation was not uncommon.

Lengthy delays in issuing visas are now routine, they said, particularly for those involved in sensitive scientific and technical fields.

The visa snag angered organizers of the annual meeting of the International Cryptology Conference, who argued that restrictions originally created to prevent the transfer of advanced technologies from the United States are now having the opposite effect.

"It's not a question of them stealing our jobs," said Stuart Haber, a Hewlett-Packard computer security expert who is program chairman for the meeting, Crypto 2005, being held this week in Santa Barbara. "We need to learn from them, but we are shooting ourselves in the foot."

Mr. Haber and other researchers stressed that progress is made in the field of cryptography by continually investigating existing algorithms and systems for weaknesses, in efforts like Ms. Wang's. Among scholars and software engineers, finding such obscure logical flaws is considered a badge of honor and not a hostile act.

Ms. Wang, a mathematician at Tsinghua University in Beijing, and her student Hongbo Yu were scheduled to present a paper in Santa Barbara on Monday on their successful attack on a United States government cryptographic function called Sha-1.

Sha-1 is a formula for creating what mathematicians call a hash, a single number used to represent a larger message or a data file. Such algorithms are routinely used in encryption and

authentication systems.

In addition to presenting the technical paper, Ms. Wang had been planning on detailing further advances in her work during an informal session this week, according to several researchers attending the event.

After Ms. Wang failed to obtain a visa, a third member of the research team, Yiqun Lisa Yin, presented the paper instead on Monday morning. A Chinese citizen, she is currently an independent security consultant in Connecticut and has been a student of Ronald L. Rivest, a prominent M.I.T. cryptographer.

An official at the National Institute for Standards and Technology, which is responsible for maintaining the country's cryptographic standards, said that he was disappointed by Ms. Wang's absence and that he had tried to intervene several times in recent weeks to persuade the State Department to allow her to appear at the conference.

"I have no idea why she didn't get her visa," said the official, William Burr, the manager of the Security Technology Group at the institute. "But I attempted to convince them that this wasn't some strange woman. I wanted to let them know that there was someone whose business was affected by her work and who was anxious to see her."

He said he was still hopeful that Ms. Wang would be permitted to attend a technology conference that the institute has scheduled for October.

A State Department spokeswoman said on Monday that the potential time it takes for visa applications to be approved is clearly outlined on Web sites maintained by United States embassies around the world.

"I certainly do appreciate that this is a frustration," said the spokeswoman, Angela Aggeler, of the Bureau of Consular Affairs. "We talk to people who experience this all the time."

She noted that Chinese visas that require review under a scientific and technical category, known as Mantis (as in praying mantis), routinely take more than two months. Ms. Wang and her student both applied in early July. Ms. Wang was interviewed by consular officials on Aug. 9, but typically two weeks are needed after such an interview for a visa to be processed.

Last week, after the conference organizers realized that it was unlikely that Ms. Wang would obtain a visa in time to attend the event, they contacted the White House science adviser, John H. Marburger III, asking him to intervene with the State Department. (Asked if he had done so, Mr. Marburger's office said only that such questions are routinely referred to the Office of Consular
Affairs.)

The organizers noted that another Chinese computer security expert, Dingyi Pei, a researcher at the State Key Laboratory of Information Security in Beijing and head of the International Cryptology Conference's annual Asia research conference, had not received a visa last year. Because of the delay last year, he applied this year in early June and had his interview July 19, but did not get a visa until Tuesday.

URL: http://www.nytimes.com

LOAD-DATE: August 17, 2005

THE NATIONAL COUNTERINTELLIGENCE STRATEGY OF THE UNITED STATES, SUBMITTED BY THE HONORABLE MICHELLE VAN CLEAVE, NATIONAL COUNTERINTELLIGENCE EXECUTIVE, OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

The National Counterintelligence Strategy of the United States

Office of the National Counterintelligence Executive

March 2005

National Counterintelligence Strategy of the United States

PREFACE

The Counterintelligence Enhancement Act of 2002 (50 USC 401) directs that the Office of the National Counterintelligence Executive produce, on an annual basis, a strategy for the counterintelligence programs and activities of the United States Government. This is the first national counterintelligence strategy promulgated pursuant to that Act. President George W. Bush approved *The National Counterintelligence Strategy of the United States* on March 1, 2005.

Counterintelligence, as defined in the National Security Act of 1947, is "information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations or foreign persons, or international terrorist activities."

As used in this *Strategy*, counterintelligence includes defensive and offensive activities conducted at home and abroad to protect against the traditional and emerging foreign intelligence threats of the 21st Century.

TABLE OF CONTENTS

PREFACE i

INTRODUCTION 1

COUNTERINTELLIGENCE AND NATIONAL SECURITY 3

I. We will extend the safeguards of strategic counterintelligence to the Global War on Terrorism. 3

II. U.S. counterintelligence will shift from a reactive posture to a proactive strategy of seizing advantage. 4

III. U.S. counterintelligence will help protect the sensitive technologies that are the backbone of our security. 5

IV. U.S. counterintelligence will safeguard the integrity of intelligence operations and analysis, and defeat foreign intelligence operations. 6

V. U.S. counterintelligence will seek to ensure a level economic playing field so that business and industry are not disadvantaged by foreign intelligence operations. 6

VI. The intelligence community will ensure that counterintelligence analytic products are available to the President and his national security team to inform decisions. 7

BUILDING A NATIONAL COUNTERINTELLIGENCE SYSTEM 9

CONCLUSION 13

INTRODUCTION

The National Security Strategy of the United States seeks to defend the peace by fighting terrorists and tyrants, to preserve the peace by building good relations among the great powers, and to extend the peace by encouraging free and open societies on every continent.

These fundamental objectives of our great Nation are not easily won. The terrorists and tyrants, the opponents of peace and freedom, are not passively watching from the sidelines. They are actively engaged in efforts to undermine the United States and our allies, and these efforts include some dimension of intelligence activities directed against us. Specifically, foreign adversaries seek to:

- penetrate, collect, and compromise our national security secrets (including sensitive information, plans, technology, activities, and operations) to advance their interests and defeat United States objectives.
- manipulate and distort the facts and reality presented to United States policy-makers by manipulating the intelligence we gather, and by conducting covert influence operations.
- detect, disrupt and counter national security operations including clandestine collection and special activities, special operations, other sensitive intelligence, and military and diplomatic activities.
- acquire critical technologies and other sensitive information to enhance their military capabilities or to achieve an economic advantage.

Collectively, these foreign intelligence activities present a threat to the Nation's security and prosperity. The United States requires national, systematic, and well-defined policies to counter them. A key to success in defeating these threats is a strategic counterintelligence response that supports the National Security Strategy.

The National Counterintelligence Strategy of the United States has four essential objectives:

- Identify, assess, neutralize, and exploit the intelligence activities of foreign powers, terrorist groups, international criminal organizations, and other entities who seek to do us harm.
- Protect our intelligence collection and analytic capabilities from adversary denial, penetration, influence, or manipulation.

- Help enable the successful execution of our sensitive national security operations.
- Help safeguard our vital national security secrets, critical assets, and technologies against theft, covert foreign diversion, or exploitation.

To achieve these objectives, we will draw upon the full range of counterintelligence capabilities including counterespionage, counter-deception, and offensive operations against hostile intelligence activities. Each of these national security tools must be strategically driven and employed to protect the United States from foreign threats, and to advance our national interests.

This document sets forth the national counterintelligence strategy of the United States in the context of our broad national security objectives and the foreign intelligence threats we face.

COUNTERINTELLIGENCE AND NATIONAL SECURITY

America faces substantial challenges to its security, freedom and prosperity. To meet them we must defeat global terrorism, counter weapons of mass destruction, ensure the security of the homeland, transform defense capabilities, foster cooperation with other global powers, and promote global economic growth. Our ability to meet these challenges is threatened by the intelligence activities of traditional and non-traditional foreign powers. Foreign intelligence services and others (e.g., terrorists, foreign criminal enterprises, cyber intruders, etc.) use clandestine activities and operations to harm and disadvantage U.S. national security interests. Counterintelligence is a key strategic national security tool that we use to defeat these foreign threats.

I. We will extend the safeguards of strategic counterintelligence to the Global War on Terrorism.

During the Cold War, our adversaries gained access to vital secrets of the most closely guarded institutions of our national security establishment. These included the clandestine, technical, and analytic directorates of the CIA; the counterintelligence division of the FBI; sensitive National Security Agency operations; Naval intelligence operations; nuclear weapons information; cryptographic keys for our secure communications; operational war plans for the defense of Europe; and plans for ensuring the survival of United States leadership in the event of war.

These peacetime losses resulted in grave damage in terms of secrets compromised, intelligence sources and methods degraded, and lives lost. Moreover, these compromises could have had even greater consequences had we been forced to go to war. Today we are engaged in a war on terrorism which has invaded our shores and threatens Americans around the globe. In this war, the potential consequences of counterintelligence failures are more immediate than during the Cold War, and put in jeopardy our combat operations, deployed forces, intelligence officers, diplomats, and other U.S. citizens.

Terrorist groups gain significantly when they have the support of state sponsors, which means that the intelligence services of these regimes can be links in the global terrorist support network. In Afghanistan and Iraq, we have seen limited examples where enemy intelligence operations have enabled terrorists to target Americans. In addition, Al Qaida and other terrorist organizations have employed classic intelligence methods to gather information, recruit sources, and run assets. In order to operate clandestinely, terrorist groups often act like intelligence organizations by conducting pre-operational planning, compartmented operations, covert communications, and training. The global

war on terrorism requires an effective counterintelligence strategy to help counter these hostile activities.

II. U.S. counterintelligence will shift from a reactive posture to a proactive strategy of seizing advantage.

If the purpose of intelligence operations and analysis is to understand an adversary's plans and intentions, the purpose of counterintelligence is to be aware of and exploit the adversary's intelligence operations. We need to be aggressive and creative in exposing the activities of foreign intelligence services. Utilizing a proactive counterintelligence strategy can help identify specific intelligence collection techniques, and gauge an appropriate response to counter the interests of an adversary. This requires a tighter coupling between organizations that collect foreign intelligence, and counterintelligence organizations, in order to fully exploit collection, analysis, and offensive operations. We need to incorporate counterintelligence considerations into strategic and tactical planning, operations, and training. The Intelligence Reform and Terrorism Prevention Act of 2004, which created a Director of National Intelligence, with a National Counterintelligence Executive under the Director, takes a significant step toward increasing community-wide coordination.

Since 1985, nearly 80 Americans have been arrested for crimes related to passing classified information to foreign governments. These spies were able to operate undetected for too long with disastrous results.

- The Walker ring in the Navy – over 17 years.
- The Conrad group in the U.S. Army – over 18 years.
- The Ames case in CIA – over 9 years.
- The Hanssen case in the FBI – over 21 years.
- The Montes case in DIA – over 15 years.

Although each of these cases represents an individual success in terms of a criminal prosecution, taken as a whole they reveal a larger systemic vulnerability in our national security. In the past, a comprehensive focus was lacking in the intelligence community's approach to protecting secrets. The counterintelligence mission must be transformed into a more coordinated, community-wide effort to help neutralize penetrations of our government. Within the United States, we must transform both our operational and analytical focus from a case-driven approach to a more strategic assessment of an adversary's presence, capabilities and intentions. Strategic

4 National Counterintelligence Strategy of the United States

counterintelligence analysis must drive operations. This requires looking beyond customary targets, such as known intelligence officers, to a larger population of foreign visitors and others whose activities suggest they might be involved in intelligence collection activities against the United States.

III. U.S. counterintelligence will help protect the sensitive technologies that are the backbone of our security.

The U.S. national defense strategy is based on a continuous transformation that utilizes cutting-edge capabilities, and places a premium on sensitive technologies that provide an advantage. Plans that ensure strategic superiority can be jeopardized if essential secrets are stolen and incorporated into an adversary's weapons systems. The United States spends billions of dollars developing weapons systems, which often rest on essential technological secrets. If foreign intelligence services steal these technological secrets, both our resource investment and our national security advantage are lost.

Today, more than 90 countries target sensitive U.S. technologies. Many employ collection techniques that extend beyond simple clandestine operations, and include tasking visiting businessmen, scientists, foreign students, trade shows, and debriefing visitors upon their return home. Counterintelligence planning and execution must proceed from a national counterintelligence strategy and be an inherent part of the mission at research laboratories, defense establishments, and with partners in industry. Counterintelligence and security considerations should not be an afterthought imposed on scientists, researchers, and those who develop sensitive technology. Coordinated and integrated counterintelligence information and analysis will be made available to senior government leaders, and, when appropriate, to security managers in the private sector.

Comprehensive risk management, valid security practices, and an informed strategic worldview are among the best guarantors of success against foreign intelligence threats. We will reach out to the private sector, especially those in the science and technology community, to increase intelligence threat awareness by providing threat information, and educating these audiences to the variety of ways our adversaries acquire and steal information.

The departments and agencies charged with protecting the homeland are building new channels for information sharing across government, including at the state and local level, with private industry, and with foreign partners. We must ensure our adversaries do not exploit these new arrangements, which could defeat the very goal of information sharing. In the global war on terrorism, we have entered into partnerships with foreign governments and international organizations whose many views and interests may be different from our own. We must ensure that intelligence sharing is measured against potential risks and that sensitive intelligence sources, methods, and operations are safeguarded.

IV. U.S. counterintelligence will safeguard the integrity of intelligence operations and analysis, and defeat foreign intelligence operations.

Intelligence is vital to the formulation and execution of U.S. national security policy and to the Nation's security. Today, the integrity of our intelligence is increasingly challenged as adversaries seek to deny us insight into their plans and mislead our decision-makers. Therefore, ensuring the reliability of intelligence becomes a key function of counterintelligence and is a necessary precondition to its very usefulness.

Foreign intelligence services have acquired significant amounts of our classified information, including sensitive U.S. intelligence capabilities. As a result of this knowledge, some countries have become very adept at deceiving and misleading us. These foreign powers attempt to present a false picture of reality through denial and deception operations which increases our uncertainty about their capabilities and intentions. It is the goal of counterintelligence operations and analysis to pierce that false picture, and the threats posed by these adversaries.

An intelligence capability is only as strong as the counterintelligence practices that ensure its integrity. Significant failures in counterintelligence can result in significant failures in positive or foreign intelligence. For example, while a given collection system may yield a wealth of intelligence, it may be useless and misleading if it has been corrupted to show only what an adversary wants us to see. While there are no guarantees that our intelligence collection efforts and our analysis are always accurate, we must establish rigorous procedures to help ensure the integrity of the intelligence that reaches decision-makers. Counterintelligence can supply techniques by which the reliability of a collection system, the *bona fides* of an asset, or the accuracy of an analytic judgment can be validated to ensure its integrity.

V. U.S. counterintelligence will seek to ensure a level economic playing field so that business and industry are not disadvantaged by foreign intelligence operations.

The United States is a nation of commerce and we value the freedom of trade as both a personal liberty and a cornerstone of national wealth. However, if adversaries can exploit the technological accomplishments of industry and gain an unfair advantage, not all trade inures to the Nation's good. While most foreign economic competition is open and lawful, it is not exclusively so. Some business competitors, supported by foreign intelligence services, employ classic intelligence methods in an attempt to gain an advantage over American companies. The outflow of sensitive trade secrets and proprietary information erodes our comparative economic advantage, and undermines national security. Foreign companies that unlawfully acquire U.S. technology are able to

compete unfairly against U.S. firms, which bear heavy research and development costs associated with innovative technology.

As our economy moves toward dependency on the benefits of information technology and networked data systems, our economic well-being and our national security could become vulnerable to foreign intelligence intrusion and manipulation of our cyber systems. We must ensure that we identify, understand, and counter these threats.

We will seek to identify foreign intelligence operations conducted against U.S. business and industry and we will provide the appropriate threat information to enable them to take such risk mitigation measures as they deem prudent.

VI. The intelligence community will ensure that counterintelligence analytic products are available to the President and his national security team to inform decisions.

To the extent we can observe them, the intelligence activities of foreign powers are a window into their respective interests and plans. Insights into the foreign intelligence activities of others can confirm or shape the prospects for cooperation. Effective counterintelligence analysis can connect the seemingly detached, illuminate hidden relationships, and reveal patterns of activity and behavior previously not observed. In this manner, counterintelligence can supply unique insights into the actions of our adversaries and the actions directed against us, as well as provide opportunities for advancing our own interests.

Counterintelligence represents a philosophic approach that can help bring coherence to many areas of national policy. Effective counterintelligence and security are integral to program efficiency, combat, and operational effectiveness, and foreign policy success. For each national security program, military endeavor, and foreign policy undertaking, there should be consideration for a corresponding counterintelligence plan to help ensure success.

BUILDING A NATIONAL COUNTERINTELLIGENCE SYSTEM

The counterintelligence capabilities of the United States evolved over time to fit the shape and mission of the disparate institutions in which they are housed. The defined missions of some counterintelligence elements are non-specific, and taken together, these missions do not necessarily provide a response equal to the breadth of the threats arrayed against the United States. Together with their parent national security agencies, these counterintelligence elements must transform to meet the threats of the 21st Century.

Until recently, counterintelligence was an enterprise with no single leadership voice. The counterintelligence community's structure was fragmented and too tactically oriented to provide comprehensive protection to the Nation. The community was not designed to accomplish a strategic mission; rather, the various counterintelligence elements were part of a loose confederation of independent organizations with narrow and differing responsibilities, jurisdictions, and capabilities. Operations tended to focus on individual cases and were conducted with insufficient strategic overview of the potential impact of a synergistic effort.

In the future, each member of the counterintelligence community must be prepared to assume new responsibilities, and join together in a unity of effort, as the *National Counterintelligence Strategy* matures. To be effective, the *National Counterintelligence Strategy* requires that essential processes and features be inculcated into government structures and business models. A national system is needed to integrate, direct, and enhance United States counterintelligence in support of national security decision-making. The features of the National Counterintelligence System include:

National policy leadership and strategic direction. The Director of National Intelligence and the National Counterintelligence Executive, supported by the National Counterintelligence Policy Board, will chart the national counterintelligence mission and will direct and coordinate the resources of the counterintelligence community to accomplish a number of national-level goals including:

- A national program for counterintelligence activities that is strategic, coordinated, and comprehensive in understanding foreign intelligence threats.
- An array of strategic counterintelligence operational and informational options in foreign and defense policy for the President and his national security leadership team.
- A comprehensive assessment and description of foreign intelligence threats and risks to United States national security interests.

- The allocation of counterintelligence community resources prioritized against risk and opportunity.

- Specific counterintelligence policies for attacking foreign intelligence services systematically via strategic counterintelligence operations.

Facilities for cross-agency and cross-disciplinary work. Executing the national counterintelligence mission requires the careful orchestration and integration of many centers of analytic and operational expertise throughout the government. The Director of National Intelligence and the National Counterintelligence Executive will examine the need to establish a national counterintelligence center to integrate threat data, refine collection requirements, and provide a basis for initiating and supporting counterintelligence operations.

Damage assessment process. When national security secrets are lost through espionage or other disclosures, we must assess the loss and impact in order to mitigate damage. In the past, damage assessments received too limited a distribution because of security concerns. We must apply the lessons learned from damage assessments to ensure future vulnerabilities are mitigated. This will require the counterintelligence community take a more centralized approach to these assessments. We will improve the process to support more timely and thorough damage assessments, and ensure the findings are made available to decision-makers with relevant responsibilities.

Resources and performance measurement. The success of any intelligence initiative, sensitive technology development, or national security program depends in part on effective counterintelligence and security. In the past, counterintelligence support was viewed as an unfunded or underfunded mandate with little consideration of requirements or costs. The planning and budgeting processes should ensure that dedicated funding for counterintelligence and security requirements is integrated into sensitive plans and programs. We should seek to ensure the best use of resources is measured against the *National Counterintelligence Strategy* by including performance metrics to chart progress against strategic goals and objectives.

Training and standardization of the counterintelligence cadre. The training and education of collectors, analysts, investigators, and operators in the counterintelligence community has not always been equal to the performance we have demanded of them. The complexity of this subject requires a mastery of many disciplines and skills. The counterintelligence profession needs a set of common standards across many counterintelligence missions. We need to reach across departments and agencies to find centers of training excellence, address deficiencies, and upgrade the availability and uniformity of training.

Intelligence warning process. The discipline of counterintelligence, with its focus on patterns of and anomalies in activities and behaviors, can provide unique insights into foreign intelligence capabilities and intentions. We must ensure the perspectives gained from counterintelligence operations and analysis are incorporated into the intelligence indication and warning process.

CONCLUSION

At the dawn of the 21st Century, the prospects for freedom, peace and prosperity have never been brighter. Yet we are a Nation at war, and we have suffered grievous attacks on our homeland. The threats we face are grave and diverse, and the intelligence threats that accompany them are equally complex. To respond to these threats, *The National Counterintelligence Strategy of the United States* calls for a proactive response utilizing all of our counterintelligence resources.

The components of this strategic response include:

- improvements to each of our counterintelligence capabilities to meet the range of foreign intelligence threats: human, technical and cyber.
- all-source counterintelligence analysis and strategic planning to drive operations in order to identify, assess, neutralize and exploit foreign intelligence activities before they can do harm to the United States.
- coordination, integration, and strategic orchestration of the activities of the counterintelligence elements of the government.
- counterintelligence support to, and involvement by, all national security policy elements of the government.

REVISED PREPARED STATEMENT OF DR. LARRY M. WORTZEL, VISITING FELLOW, THE HERITAGE FOUNDATION

Mr. Chairman, Members of the Committee,

Thank you for the opportunity to testify today on the theft of national security sensitive technology in the United States. As a former military intelligence officer who has tracked the activities of the People's Liberation Army and Chinese intelligence services for 35 years, I know of no more pervasive and active intelligence threat to America's national security than that posed by the People's Republic of China. The work force available to the Chinese government and its corporations to devote to gathering information in the United States is nearly limitless. There are some 700,000 visitors to the United States from China each year, including 135,000 students. It is impossible to know if these people are here for study and research or if they are here to steal our secrets. The sheer numbers defy complete vetting or counterintelligence coverage.

In 2003, for example, the State Department granted about 27,000 visas to Chinese "specialty workers," the H1-B visa. Some of these were intra-company transfers coming to the United States from US firms operating in China. Between 1993 and 2003, the United States has granted an average of 40,000 immigrant visas to Chinese each year. The sheer magnitude if these numbers presents a great challenge to the Federal Bureau of Investigation, particularly when the US is also concerned about terrorism, which occupies a lot of investigative time for agents.

The Chinese People's Liberation Army and the defense establishment in China started programs in the late 1970s and 1980s to create companies designed to bring in needed defense technology; the goal was to produce defense goods for the PLA and for sale to other countries. The General Political Department of the People's Liberation Army started a proprietary company, *Kaili*, or Kerry Corporation, that for years operated in the U.S. as a real estate and investment company. The General Equipment Department of the PLA operated a proprietary company, Polytechnologies, or *Baoli*, that had offices here in the U.S. In addition, the General Logistics Department operated a proprietary called *Xinshidai*, or New Era, that had offices in our nation and continues to be responsible for a network on PLA manufacturing plants in China. These technically are independent legal entities under Chinese law, but the Central Military Commission of the Chinese Communist Party established them to serve the interests of the PLA and the military industrial complex. Active or retired officers of the PLA or their families originally staffed these companies. The PLA and related defense science and technology research and development organizations in China regularly operate trade fairs to attract American high technology into China.

The Deputy Undersecretary of Defense for Technology Security and Counterproliferation has testified that there are between 2,000 and 3,000 Chinese front companies operating in the United States to gather secret or proprietary information, much of which is national security technology or information. The deputy director of the Federal Bureau of Investigation for counterintelligence recently put the number of Chinese front companies in the U.S. at over 3,200. Many of these front companies are the spawn of the military proprietary companies discussed in the preceding paragraph.

The nature of the Chinese state complicates the problem of knowing what the large numbers of travelers and students from China are actually doing. China is still an authoritarian, one-party state led by the Chinese Communist Party with a pervasive intelligence and security apparatus. The Chinese government is able to identify potential collectors of information and, if necessary, to coerce them to carry out missions on behalf of the government because of the lack of civil liberties in China. Let me quote the first three sentences of Chapter 1, Article 1, of the Chinese Constitution: "The People's Republic of China is a socialist state under the people's democratic dictatorship led by the working class and based on the alliance of workers and peasants. The socialist system is the basic system of the People's Republic of China. Disruption of the socialist system by any organization or individual is prohibited."

The People's Republic of China is methodical in its programs to gather information from abroad. In March 1986, the PRC launched a national high technology research and development program with the specific goal of benefiting China's medium and long-term high technology development. This centralized program, known as the "863 Program" for the date when it was announced, allocates money to experts in China to acquire and develop bio-technology, space technology, information technology, laser technology, automation technology, energy technology and advanced materials. The 863 program was proposed by China's strategic weapons scientists to emphasize strategic civil and military technology development. Thousands

of students and scientists were sent abroad by China over the years to pursue critical civil and military, dual-use technologies. This practice still continues. When I was at the American Embassy in China and conducted due diligence checks to confirm the nature of Chinese companies seeking to do high technology business in the United States I most often found that the address identified for a company on a visa application turned out to be a People's Liberation Army or PRC government defense research institute. Thus, the United States faces an organized program out of China that is designed to gather high technology data and equipment of military use.

My colleague today, Mr Maynard Anderson, will discuss some of the ways that our government and industry can defend against intelligence gathering by China through defensive counterintelligence and security education programs. It is also important to know that we have other programs to screen out people coming to the United States to gather our trade or military secrets. In January 1998, the VISAS MANTIS program was developed to assist the American law enforcement and intelligence communities in securing U.S.-produced goods and information that are vulnerable to theft. Travelers are subject to a world-wide name-check and vetting procedure when they apply for visas. The security objectives of this program are to prevent the proliferation of weapons of mass destruction and missile delivery systems; to restrain the development of destabilizing conventional military capabilities in certain regions; to prevent the transfer of arms and sensitive dual-use items to terrorists; and to maintain United States advantages in militarily critical technologies. This program operates effectively and can vet a Chinese student in as few as 13 days. Non-students may take longer, as many as 56 days. However, I can tell you based on my trip to China two weeks ago that the American Embassy in Beijing and the Consulate in Guanzhou are able to process and vet in about two weeks visas for non-student travelers who fully and accurately outline the purpose and itinerary of their trip. Still, many U.S. companies complain about delays in getting visas for travelers they want to bring to the United States. Automation and data-mining software can speed visa processing to ensure these companies can be competitive. The government also operates a "technology alert list" to identify legal travelers from China that may benefit from exposure to advanced U.S. technology with military application. Of course, the consular officers manning visa lines in embassies must be trained to look for signs of espionage for screening to be effective.

Many provinces and municipalities in China now operate high technology zones and "incubator parks" specifically designed to attract back Chinese nationals who have studied or worked overseas in critical high technology areas. When students or entrpreneurs return with skills or knowledge that the central government deems critical they are given free office space in the parks, loans, financial aid, and administrative help in setting up a business designed to bring in foreign investment and technology. Their companies are given tax holidays. Innovative programs such as at Beijing's Zhongguancun High Technology Park and Guangzhou's High Technology Economic and Trade Zone get central government help. These are admirable programs that will develop entrpreneurial skills among well-educated Chinese citizens. However, as students and employees of U.S. companies return home, it is important to know that they are not taking back American economic or military secrets. Good counterintelligence and industrial security programs are very important to U.S. security given this threat.

Mr. Chairman, the enforcement of intellectual property protection laws in China is spotty and inconsistent at best. This is one of the major complaints of American high technology companies about China's compliance with its obligations under the World Trade Agreement. It will certainly be a subject discussed by President Bush and Chinese President Hu Jintao this week. The tendency to steal intellectual property and high technology secrets in China is worsened when intellectual property laws are not enforced there. And the problem is further exacerbated when centralized Chinese government programs, such as the "863 Program" I mentioned earlier in my testimony, are specifically designed to acquire foreign high techology with military application. This only creates a climate inside China that rewards stealing secrets.

I believe that U.S. government security, intelligence and law enforcement agencies must focus on the national security. They should be looking for acts of espionage and for violations of the Arms Export Control Act or the Export Administration Act. When it comes to corporate or industrial espionage that is not a matter of national security, I believe that the government owes American companies a good legal infrastructure to protect trademarks, patents and copyrights; a system of education on industrial security; and a strong effort to ensure that China meets its own obligations to create a rule of law that protects the right of ownership and intellectual property. However, I do not believe that American intelligence or security agencies should focus on forms of economic espionage that do not involve national secu-

rity information. From the standpoint of Congressional action, my view is that the Congress should reconsider the Export Administration Act with a view toward ensuring that its provisions meet the needs of 21st century technology. The 1979 Export Administrtion Act expired in 2001. The Senate passed a new Act in 2001, but no revision passed the House. And the Executive Branch must regularly review the Commodity Control List to ensure that appropriate national security controls on exports protect the nation's security but do not unduly restrict the ability of American industry to compete in the world market. Generally, technologies that are widely available on the world market and not unique to the United States should not be unduly restricted unless they can be subject to mulitlateral export controls.

Finally, we cannot become paranoid and suspect that every traveler, student and businessman from China is a spy or is out to steal technology. Many of the people that come to the United States absorb our values and bring them home. We must keep in mind that in earlier decades, in places like the Republic of China on Taiwan and in South Korea, the steady flow of returning students and immigrants who were exposed to American values and principles eventually eroded dictatorships and produced multi-party democracies. The prudent course of action for the United States is to maintain law enforcement programs, counterintelligence programs, security education and industrial security programs as the means to protect our nation.

Thank you for your invitation to testify today.